「暗号アルゴリズム実装試験ツールの機能追加(GCM/XTS/鍵確立手法)」に係る一般競争入札

入 札 関 係 書 類

I．入札説明書
II．入札説明書別添（契約書案、その他関係資料）
III．仕様書
IV．入札資料作成要領及び評価手順
V．評価項目一覧

2010年11月18日

独立行政法人 情報処理推進機構

I. 入 札 説 明 書

独立行政法人 情報処理推進機構の請負契約に係る入札公告（2010年11月18日付け公示）に基づく入札については、関係法令及び独立行政法人 情報処理推進機構入札心得に定めるもののほか下記に定めるところによる。

記

1. 競争入札に付する事項

(1) 作業の名称　暗号アルゴリズム実装試験ツールの機能追加(GCM/XTS/鍵確立手法)
(2) 作業内容等　III.仕様書のとおり。
(3) 履 行 期 限　III.仕様書のとおり。
(4) 入 札 方 法　入札金額は、暗号アルゴリズム実装試験ツールの機能追加(GCM/XTS/鍵確立手法)に関する総価で行う。総価には、それぞれの業務にかかる費用をすべて含むものとする。
なお、本件については入札の際に提案書を提出し、技術審査を受けなければならない。落札決定に当たっては、入札書に記載された金額に当該金額の5パーセントに相当する額を加算した金額（当該金額に1円未満の端数が生じたときは、その端数金額を切捨てるものとする。）をもって落札価格とするので、入札者は消費税及び地方消費税に係る課税事業者であるか免税事業者であるかを問わず、見積った契約金額の105分の100に相当する金額を入札書に記載すること。
また、入札者は、その提出した入札書の引き換え、変更又は取り消しをすることはできないものとする。

2. 競争参加資格

(1) 予算決算及び会計令（以下「予決令」という。）第70条の規定に該当しない者であること。なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別の理由がある場合に該当する。
(2) 予決令第71条の規定に該当しない者であること。
(3) 法人税、消費税及び地方消費税について、納付期限を過ぎた未納税額がないこと。
(4) 登記簿謄本、営業経歴書及び財務諸表を提出すること。または、平成22･23･24年度競争参加資格（全省庁統一資格）における資格を有する者であること。

3. 入札者の義務

この入札に参加を希望する者は、当機構が交付する仕様書に基づいて提案書を作成し、これを入札書に添付して入札書の受領期限内に提出しなければならない。また、開札日の前日までの間において当機構から当該書類に関して説明を求められた場合は、これに応じなければならない。なお、入札者の作成した提案書は当機構において審査するものとし、採用し得ると判断した提案書を添付した入札書のみを落札決定の対象とする。

4. 入札説明会の日時及び場所

(1) 入札説明会の日時
2010年11月24日（水）14時00分
(2) 入札説明会の場所
東京都文京区本駒込2-28-8　文京グリーンコートセンターオフィス13階
独立行政法人 情報処理推進機構　会議室A
※ 入札説明会への参加を希望する場合は、15.(4)の担当部署まで電子メールにより申し込むこと。

5. 入札に関する質問の受付等

(1) 質問の方法
質問書（様式1）に所定事項を記入の上、電子メールにより提出すること。

(2) 受付期間
2010年11月19日（金）から2010年12月3日（金）17時00分まで。
なお、質問に対する回答に時間がかかる場合があるため、余裕をみて提出すること。

(3) 担当部署
15.(4)のとおり

(4) 既存システムの設計資料の開示
提案書を提出しようとする者が既存システムの設計仕様書、ソースコードの閲覧を希望する場合は、当機構が用意する閲覧場所において、当機構職員の立会の下に閲覧することができるので、事前に15.(4)の担当部署へ電子メールで連絡すること。
なお、閲覧期間は2010年11月19日(金）から2010年12月3日（金）までの10時00分から17時00分(12時30分～13時30分の間は除く)までの間の1時間程度とする。

6. 入札書等の提出方法及び提出期限等

(1) 受付期間
2010年12月6日（月）から2010年12月10日（金)。
持参の場合の受付時間は、月曜日から金曜日(祝祭日は除く)の10時00分から17時00分(12時30分～13時30分の間は除く）とする。

(2) 提出期限
2010年12月10日（金）17時00分必着。
上記期限を過ぎた入札書等はいかなる理由があっても受け取らない。

(3) 提出先
15.(4)のとおり。

(4) 提出書類一覧

No.	提出書類	仕様様式	部数
①	委任状（代理人に委任する場合に限る）	様式 2	1 通
②	入札書	様式 3	1 通
③	最新の納税証明書（その 3 の 3・「法人税」及び「消費税及地方消費税」について未納税のない証明用）の原本又は写し	－	1 通
④	○ 登記簿謄本（商業登記法第 6 条第 5 号から第 9 号までに掲げる株式会社登記簿等の謄本)、営業経歴書（会社の沿革、組織図、従業員数等の概要、営業品目、営業実績及び営業所の所在状況を含んだ書類）及び財務諸表類（直前 1 年間の事業年度分に係る貸借対照表、損益計算書及び株主資本等変動計算書）の原本又は写し ○ 又は平成 22･23･24 年度競争参加資格（全省庁統一資格）における資格審査結果通知書の写し	－	1 部
⑤	提案書受理票	様式 4	1 通
⑥	提案書（別紙を含む）	－	印刷物 4 部
⑦	提案書（別紙を含む）の電子ファイルが保存された媒体	－	1 部
⑧	添付資料	Ⅳ. 応札資料作成要領参照	4 部
⑨	評価項目一覧	Ⅴ. 評価項目一覧	4 部
⑩	補足資料（提出は任意）	－	4 部

(5) 提出方法

① 提出書類を持参により提出する場合
　入札書を封筒に入れ封緘し、封皮に氏名（法人の場合は商号又は名称）、宛先（15.(4)の担当者名）を記載するとともに「暗号アルゴリズム実装試験ツールの機能追加(GCM/XTS/鍵確立手法) 一般競争入札に係る入札書在中」と朱書きし、その他提出書類一式と併せ封筒に入れ封緘し、その封皮に氏名（法人の場合はその商号又は名称）、宛先（15.(4)の担当者名）を記載し、かつ、「暗号アルゴリズム実装試験ツールの機能追加(GCM/XTS/鍵確立手法) 一般競争入札に係る提出書類一式在中」と朱書きすること。

② 提出書類を郵送（書留郵便）により提出する場合
　二重封筒とし、表封筒に「暗号アルゴリズム実装試験ツールの機能追加(GCM/XTS/鍵確立手法) 一般競争入札に係る提出書類一式在中」と朱書きし、中封筒の封皮には直接提出する場合と同様とすること。

(6) 提出後
①提出書類を受理した場合は、提案書受理票を入札者に通知する。なお、受理した提案書を含む提出書類は評価・開札結果に関わらず返却しない。

7. 開札の日時及び場所

(1) 開札の日時
2010年12月17日（金）11時00分

(2) 開札の場所
東京都文京区本駒込2-28-8 文京グリーンコートセンターオフィス13階
独立行政法人 情報処理推進機構 会議室B

8. その他の事項については、独立行政法人 情報処理推進機構入札心得の定めにより実施する。

9. 入札の無効

　入札公告に示した競争参加資格のない者による入札及び入札に関する条件に違反した入札は無効とする。

10. 落札者の決定方法
　独立行政法人情報処理推進機構会計規程第29条の規定に基づいて作成された予定価格の制限の範囲内で、当機構が入札説明書で指定する要求事項のうち、必須とした項目の最低限の要求をすべて満たしている提案をした入札者の中から、当機構が定める総合評価の方法をもって落札者を定めるものとする。ただし、落札者となるべき者の入札価格によっては、その者により当該契約の内容に適合した履行がなされないおそれがあると認められるとき、又はその者と契約することが公正な取引の秩序を乱すこととなるおそれがあって著しく不適当であると認められるときは、予定価格の範囲内の価格をもって入札をした他の者のうち、評価の最も高い者を落札者とすることがある。

11. 入札保証金及び契約保証金
　全額免除

12. 契約書作成の要否
　要（別添の契約書（案）を参照）

13. 支払の条件
　契約代金は、最終納入の完了後、当機構が適法な支払請求書を受理した日の属する月の翌月末日までに契約金額を支払うものとする。

14. 契約者の氏名並びにその所属先の名称及び所在地
〒113-6591　東京都文京区本駒込2-28-8 文京グリーンコートセンターオフィス16階

独立行政法人 情報処理推進機構 理事長 藤江 一正

15. その他

(1) 競争参加者は、提出した証明書等について説明を求められた場合は、自己の責任において速やかに書面をもって説明しなければならない。

なお、提出された書類をもとにヒアリングを実施する予定である。ヒアリング時のプレゼンテータは、プロジェクトマネージャであることが必要である。また、担当技術者をヒアリングに同席させること。

ヒアリングの予定日: 2010年12月14日 (火)(予備日 12月15日 (水))

(2) 入札結果は、落札者等について当機構のウェブサイトにて公表するものとする。

(3) 落札者は、契約締結時までに入札内訳書を提出するものとする。

(4) 入札説明会への参加申込み、仕様書に関する照会先、入札に関する質問の受付、入札書類の提出先

〒113-6591

東京都文京区本駒込2-28-8 文京グリーンコートセンターオフィス16階

独立行政法人 情報処理推進機構 セキュリティセンター 情報セキュリティ認証室 担当: 橋本、櫻井

TEL: 03-5978-7545

E-mail: isec-kobo-2010@ipa.go.jp

なお、来訪する場合は、文京グリーンコートセンターオフィス13階、当機構総合受付にお越し下さい。

(5) 入札行為に関する照会先

独立行政法人 情報処理推進機構 財務部 管理グループ 担当: 日向、高橋

TEL：03-5978-7502

E-mail: itaku@ipa.go.jp

16.入札説明書に係る様式一覧

(様式1): 質問書
(様式2): 委任状
(様式3): 入札書
(様式4): 提案書受理票

（様　式　1）

年　　月　　日

独立行政法人　情報処理推進機構　理事長　殿

質　問　書

「暗号アルゴリズム実装試験ツールの機能追加(GCM/XTS/鍵確立手法)」に関する質問書を提出します。

法人名	
所属部署名	
担当者名	
電話番号	
E-mail	

質問書枚数
枚中 枚目

＜質問箇所について＞

資料名	例）　○○書
ページ	例）　P○
項目名	例）　○○概要
質問内容	

備考

1. 質問は、本様式1枚につき1問とし、簡潔にまとめて記載すること。
2. 質問及び回答は、IPA のホームページに公表する。（電話等による個別回答はしない。）また、質問者自身の既得情報（特殊な技術、ノウハウ等）、個人情報に関する内容については、公表しない。

（様　式　2）

年　　月　　日

独立行政法人　情報処理推進機構　理事長　殿

所　在　地

商号又は名称

代 表 者 氏 名　　印

委　任　状

私は、下記の者を代理人と定め、「暗号アルゴリズム実装試験ツールの機能追加(GCM/XTS/鍵確立手法)」に関する一切の権限を委任します。

代 理 人 氏 名

代理人使用印鑑

（様　式　3）

年　　月　　日

独立行政法人　情報処理推進機構　理事長　殿

所　在　地

商号又は名称

代表者氏名　　印

（又は代理人、復代理人氏名）

印

※代理人又は復代理人が入札する場合は、代表者印は特に必要としない。

入　札　書

入札金額　　¥＿＿＿＿＿＿＿＿＿＿＿＿

入札事項　　暗号アルゴリズム実装試験ツールの機能追加(GCM/XTS/鍵確立手法)

契約条項の内容及び貴機構入札心得を承知の上入札いたします。

（様　式　4）　**提案書受理票**

提案書受理票（控）

提案書受理番号

件名：「暗号アルゴリズム実装試験ツールの機能追加(GCM/XTS/鍵確立手法)」に関する提案書

【入札者記載欄】

提出年月日：　　年　　月　　日
法 人 名：
所 在 地：　〒
担 当 者：　所属・役職名
氏名
TEL　　FAX
E-Mail

【ＩＰＡ担当者使用欄】

No.	提出書類	部数	有無	No.	提出書類	部数	有無
①	委任状（委任する場合）	1部		②	入札書（封緘）	1部	
③	納税証明書	1通		④	登記簿謄本等※	1部	
⑤	提案書受理票	(本紙)		-	-	-	-
⑥	提案書（別紙を含む）	4部		⑦	提案書の電子ファイルが保存された媒体	1部	
⑧	別添資料	4部		⑨	評価項目一覧	4部	
⑩	補足資料（任意）	4部					

※登記簿謄本等の原本または写し。または、資格審査結果通知書の写し。

---------- 切り取り ----------

提案書受理番号

「暗号アルゴリズム実装試験ツールの機能追加(GCM/XTS/鍵確立手法)」に関する提案書　提案書受理票

年　　月　　日

法人名　（入札者が記載）：

担当者名（入札者が記載）：　　殿

貴殿から提案された表記提案書は、受理しました。

独立行政法人　情報処理推進機構　セキュリティセンター

担当者名：　　㊞

II. 入札説明書別添 (契約書案、その他関係資料)

○○情財第○○号

「暗号アルゴリズム実装試験ツールの機能追加(GCM/XTS/鍵確立手法)」に関する開発請負契約書（案）

独立行政法人　情報処理推進機構（以下「甲」という。）と○○○○○○（以下「乙」という。）とは、別添発注仕様書及び提案書に基づく業務を甲が乙に発注し乙がこれを請負うことに関して、次のとおり契約（末尾付記の「特記事項」及び別紙２添付の「個人情報の取扱いに関する特則」を含む。以下同様）を締結する。

（用語の定義）

第１条　本契約において使用する用語は、情報産業分野に属する事業者間で通常理解されている意味内容を有するものとする。但し、以下の各号に掲げる用語については、当該各号が定めるところによる。

(1)「開発成果物」とは、別添発注仕様書及び提案書（以下、「仕様書等」という）に基づいて開発されるべき別紙１記載の各物件をいう。

(2)「本件開発業務」とは、本契約に従って開発成果物を開発する業務をいう。

(3)「改版」とは、開発成果物の内容に加除変更を加え、または異なる記述形式で記述する（アナログ／デジタル間変換、文字／音響／画像間変換等を含む）一切の行為をいう。

(4)「件外プロダクト」とは、開発成果物のうち、専ら本件業務のために新規に開発された部分（または要素）を除いたすべての部分（または要素）をいい、何人（甲また乙を含む。以下同様）かの制作にかかるものであるか否かを問わない。

(5)「ＬＰプロダクト（Legally Protected Product)」とは、件外プロダクトのうち、何人かの権利（肖像権など非財産的権利を含む）の対象となる部分（または要素）をいう。

(6)「原プロダクト」とはＬＰプロダクトのうち、別紙１記載の各物件をいう。

(7)「ＰＤプロダクト（Public Domain　Product)」とは、件外プロダクトのうち、ＬＰプロダクトを除いたすべての部分（または要素）をいう。

（開発請負）

第２条　甲は、本件開発業務を乙に発注し、乙はこれを請負う。

2　乙は、本件開発業務の遂行にあたり、次の各号のいずれかに該当するもの（原プロダクトを除く）を開発成果物中に利用する場合、事前に様式１により利用の内容を甲に提出し、その承認を得る。

(1)国内外の社会の健全な発展及び／または情報産業の振興に資するために開発成果物を広く普及する上で支障（法律上経済上の支障であって、その程度が軽微なものを除く）を生じ得べき件外プロダクト

(2) 第 11 条第１項所定の権利に基づく開発成果物の利用自体によって、対価の支払義務が生ずることとなるＬＰプロダクト

3　乙は、本件開発業務の全部を第三者に再請負させてはならない。

4　乙は、本件開発業務の一部を第三者に再請負させることができる。この場合甲は、再請負先の行為を全て乙の行為とみなし、乙に対し、本契約上の責任を問うことができる。

5　乙は、前項に基づき再請負させる場合、事前に再請負先、再請負の対価、再請負作業内容及び請負わせる理由等を書面により甲に届け出る。なお、再請負先からの見積書を添付するものとする。

6　乙が本件開発業務の全部または一部を第三者と共同で行う場合であっても、本契約との関係においては、第４項所定の再請負とみなす。

（交付資料の取扱）

第３条　乙は、本契約に基づいて甲から交付されたすべての資料を、本契約の目的の範囲内でのみ使用する。また、乙は、甲の同意なくこれら交付資料を複製しない。

（責任者の選任）

第４条　乙は、開発業務を実施するにあたって責任者を選任して甲に届け出る。

2　責任者は、開発作業の進捗状況を常に把握するとともに、甲との連絡窓口として、右各進捗状況について甲の随時の照会に応じるとともに定期的または必要に応じてこれを甲に報告するものとする。
3　乙は、第１項により選任された責任者に変更がある場合は、速やかに甲に届け出る。

（納入）
第５条　乙は、別紙１の定めるところにより、開発成果物を甲に納入する。
2　乙が納入期限（分割納入の場合は各分割納入期限）までに所定の納入をしない場合、甲は違約金として延滞日数１日につき第 10 条所定の契約金額の 1000 分の１に相当する額を徴収することができる。但し、天災その他乙の責に帰すことができない事由、又は甲が相当と認めた技術上の事由による場合は、この限りではない。

（件外プロダクトに関する告知）
第６条　乙は、開発成果物を納入する際、次の各号所定の事項の概要を記載した「件外プロダクトリスト」（様式 2）を同時に甲に提出する。なお、該当する件外プロダクトが原プロダクトのみの場合は、第３項に従う。
(1) 件外プロダクトの一覧、及びこの内で第２条第２項所定の甲の承認の対象となったものの摘示
(2) 各件外プロダクトについて、開発成果物中に占める場所（または出現形態）、及び開発成果物中への利用の方法と態様
(3) 各ＬＰプロダクトについて、権利者の名称と連絡先、権利の内容、開発成果物への利用に付された条件の有無・内容、並びにこの内で第２条第２項所定の甲の承認の対象となったものの摘示及び右承認の内容
(4) 各ＰＤプロダクトについて、再入手の方法
(5) 件外プロダクトのうち、ＬＰプロダクト及び／またはＰＤプロダクトへの該当の有無が不分明なものについて、知れたる関係者の名称と連絡先、知れたる法的関係、及び再入手の方法
(6) 上記（1）から（5）に記載の個別事実ごとに、その秘密性の有無
2　開発成果物を分割納入する場合、前項の規定は、分割納入成果物の納入ごとに準用する。
3　甲は、件外プロダクトリストの記載内容について、乙に説明を求め、関連資料の閲覧及びそのコピーの提出等を求めることができる。
4　別紙 1 中の原プロダクトの項目に該当物件の記載がある場合、当該記載と同一内容の記載がなされた件外プロダクトリストが本条に従って提出されたものとみなす。
5　件外プロダクトリストの提出がない場合は、“該当する件外プロダクトが存在しない”旨の記載がなされた件外プロダクトリストが本条に従って提出されたものとみなす。

（実地調査）
第７条　甲は、必要があると認めるときは、乙並びに本件開発業務の再請負先に対し、自らまたはその指名する第三者をして、本件開発業務の実施状況等について、報告又は資料を求め、若しくは現場（第２条第４項の再請負先を含む）に臨んで実地に調査を行うことができる。
2　前項において、甲は乙に意見を述べ、補足資料の提出を求めることができる。

（検査、及び本件開発業務の完了）
第８条　甲は、開発成果物の納入を受けた日から 30 日以内（分割納入の場合は分割納入成果物ごとに、その納入の日から 30 日以内）に、仕様書等に基づいて検査を行い、同仕様書等に定める基準に適合しない事実を発見したときは、当該事実の概要を書面によって直ちに乙に通知する。
2　前項所定の期間内に同項所定の通知がないときは、当該期間満了日をもって開発成果物（分割納入の場合は当該分割納入成果物）は同項所定の検査に合格したものとみなす。
3　本件開発業務は、すべての開発成果物が本条による検査に合格した日をもって完了したものとみなす。この場合、甲は、完了を確認するために本件開発業務の完了通知書面を乙に交付する。
4　第１項及び第２項の規定は、第１項所定の通知書面に記載された指摘事実に対し、乙が適切な修正等を行い甲に再納入する場合に準用する。

（保証）
第９条　乙は、本件開発業務が完了した日から１年間、開発成果物に発見された欠陥・作動不良その他の不具合及び／または仕様書等所定の基準との不適合を、遅滞なく無償で修正する。

2　前項の期間経過後に発見された不具合及び不適合については、乙は、随時または甲の要請あり次第、当該不具合及び不適合に関する甲所定の情報を甲に提供する。
3　乙は、次の各号を保証する。
(1) 開発成果物（分割納入の場合は当該分割納入成果物。(3) も同様）が第 2 条第 2 項を遵守して開発されていること。
(2) 件外プロダクトリストの記載内容について、それが真実であり、かつ知りたる事実を秘匿していないこと。
(3) 件外プロダクトリスト記載の法的事実関係の下で、開発成果物が何人かの著作権その他の権利を侵害していないこと。
(4) 件外プロダクトリスト記載の法的事実関係の下で、かつ情報産業の振興及び／または国内外の社会の健全な発展に資する目的に適合する限りにおいて、第 11 条第 1 項所定の権利の円滑な行使が何人かの権利（著作権法第 28 条の権利、著作者人格権、著作隣接権等を含む）によって制限を受けることがないこと。

（対価の支払）
第 10 条　甲は、第 8 条第 3 項の規定による開発業務の完了後、乙から適法な支払請求書を受理した日の属する月の翌月末日までに、対価として、別紙 1 の定めるところにより所定の契約金額を乙に支払う。

（開発成果物の権利）
第 11 条　甲は、開発成果物（分割納入の場合は当該分割納入成果物）の全部または一部について、これを改版しないでそのまま利用し、改版し、二次的著作物を生成し、それらを販売し、他人に販売を許諾し、その他現在及び／または将来において技術的に可能なあらゆる方法と態様によって商業的及び／または非商業的に利用するために必要かつ十分な法律上のすべての権利を、本件業務が完了した日（分割納入の場合は、分割納入成果物ごとに当該分割納入成果物が第 8 条第 1 項所定の検査に合格した日）から専有する。
2　前項の権利には、著作権法及び特許法所定の各権利（著作権法第 27 条及び第 28 条に定める権利を含む）のほか、将来の法改正によって創設される権利が含まれる。
3　乙は、第 1 項所定の権利に関する登録その他の手続きについて、甲に協力する。

（ＬＰプロダクトの権利）
第 12 条　甲及び乙は、次の各号を確認する。
(1) ＬＰプロダクトの権利者は、次号の場合を除き、自己のＬＰプロダクトに対して有する著作権その他の権利の内容及び行使について、本契約によって何らの影響も受けない。
(2) 乙が第 9 条第 3 項(4)所定の保証義務を履行する行為自体によって結果的に自動的かつ当然に発生している法律効果として、ＬＰプロダクトの権利者は、第 11 条第 1 項所定の権利を正当に行使する者に対して、自己のＬＰプロダクトに対して有する著作権その他の権利を原因とする法的請求を提起できない。

（責任）
第 13 条　第 9 条第 3 項 (1) または (2) に反する事実がある場合、第 10 条所定の契約金額と同額を、当該事実に対する民法第 420 条所定の損害賠償予定額と定める。
2　第 9 条第 3 項（1）に反する事実がある場合、乙は、前項に基づく損害賠償に加えて、該当する件外プロダクトの削除その他の措置（これに要する費用は乙の負担とする）について甲の指示に従う。
3　第 9 条第 3 項（3）または（4）に反する事実がある場合、乙は、これによって甲が被る損害を第 10 条所定の契約金額を上限として賠償する。
4　前項において、件外プロダクトリスト記載の事実を甲が看過したことによる甲の損害部分については、乙は責任を免除される。

（秘密保持及び個人情報）
第 14 条　甲及び乙は、相互に本契約の履行過程において知り得た相手方の秘密を他に漏洩せず、また本契約の目的の範囲を超えて利用しない。但し、甲が、法令等、官公署の要求、その他公益的見地に基づいて、必要最小限の範囲で開示する場合を除く。

2　個人情報に関する取扱いについては、別紙 2 のとおりとする。
3 前各項の規定は、本契約終了後も有効に存続する。

（契約の変更）
第 15 条　甲又は乙は、本件開発業務の実施に伴い状況が変化したり、技術上の支障が生じるなどして、仕様書等の目標を達成できず本件開発業務の全部又は一部を中止又は変更する必要があると認めた場合、本契約の変更の協議を契約の相手方に申し出ることができる。この場合、契約の相手方は、誠意をもって協議に応ずる。

（契約の解除等）
第 16 条　甲は、次の各号の一に該当する事由がある場合には、本契約を解除することができる。
(1)乙が本契約に違反した場合
(2)乙の責に帰すべき事由により、本契約を履行する見込みがないと認めるに足る客観的状況が生来した場合
(3)乙が、本契約の対価を目的外に使用するなど不適切な経理処理が行われていた場合
(4)乙が、甲に対し、本件開発業務並びに本契約が定める届出及び報告に関して、不正又は虚偽の申立てをした場合
(5)乙が、本件開発業務と同じ内容の開発業務について、国又は公共団体等から補助等の支援を受け、または受けることとなった場合
2　本契約の解除が納入（分割納入の場合は各分割納入）の後になされた場合、契約対価の支払い、権利帰属その他の法律関係は、右解除によって初めに遡って効力を失う。
3　第 1 項(3)から(5)に該当する事由がある場合、甲は、契約を解除せずに、乙に対して契約対価額の変更、支払済契約対価の全部若しくは一部の返還、及び／または損害の賠償を求めることができる。

（手続方法）
第 17 条　乙は、本契約に基づいて行う手続きについて、甲の定める様式がある場合は、これに従う。

（その他）
第 18 条　本契約中に法令の強行規定に違反して無効となる条項がある場合、当該条項は、当該強行規定が実質的に効力を失うまでの期間、当該強行規定の許容する範囲内であってかつ当該条項が意図する趣旨と最も近い内容に変更されたものとみなして、引き続き効力を存続する。
2　本契約に定めなき事項及び疑義については、甲乙双方が協議し決定する。
3　本契約に関する紛争については、東京地方裁判所を唯一の合意管轄裁判所とする。

特記事項

（談合等の不正行為による契約の解除）
第 1 条　甲は、次の各項のいずれかに該当したときは、契約を解除することができる。
1　本契約に関し、乙が私的独占の禁止及び公正取引の確保に関する法律（昭和 22 年法律第 54 号。以下「独占禁止法」という。）第 3 条又は第 8 条第 1 項第 1 号の規定に違反する行為を行ったことにより、次の各号のいずれかに該当することとなったとき
（1）独占禁止法第 49 条第 1 項に規定する排除措置命令が確定したとき
（2）独占禁止法第 50 条第 1 項に規定する課徴金納付命令が確定したとき
（3）独占禁止法第 66 条第 4 項の審決が確定したとき
（4）独占禁止法第 7 条の 2 第 13 項又は第 16 項の課徴金納付命令を命じない旨の通知があったとき
2　本契約に関し、乙の独占禁止法第 89 条第 1 項又は第 95 条第 1 項第 1 号に規定する刑が確定したとき
3　本契約に関し、乙（法人の場合にあっては、その役員又は使用人を含む。）の刑法（明治 40 年法律第 45 号）第 96 条の 3 又は第 198 条に規定する刑が確定したとき

（談合等の不正行為に係る通知文書の写しの提出）
第 2 条　乙は、前条第 1 項各号のいずれかに該当することとなったときは、速やかに、次の各号の文

書のいずれかの写しを甲に提出しなければならない。
（1）独占禁止法第 49 条第 1 項の排除措置命令書
（2）独占禁止法第 50 条第 1 項の課徴金納付命令書
（3）独占禁止法第 66 条第 4 項の審決についての審決書
（4）独占禁止法第 7 条の 2 第 13 項又は第 16 項の課徴金納付命令を命じない旨の通知文書

（談合等の不正行為による損害の賠償）
第 3 条　乙が、本契約に関し、第 1 条の各項のいずれかに該当したときは、甲が本契約を解除するか否かにかかわらず、かつ、甲が損害の発生及び損害額を立証することを要することなく、乙は、契約金額（本契約締結後、契約金額の変更があった場合には、変更後の契約金額）の 100 分の 10 に相当する金額（その金額に 100 円未満の端数があるときは、その端数を切り捨てた金額）を違約金（損害賠償額の予定）として甲の指定する期間内に支払わなければならない。
2　前項の規定は、本契約による履行が完了した後も適用するものとする。
3　第 1 項に規定する場合において、乙が事業者団体であり、既に解散しているときは、甲は、乙の代表者であった者又は構成員であった者に違約金の支払を請求することができる。この場合において、乙の代表者であった者及び構成員であった者は、連帯して支払わなければならない。
4　第 1 項の規定は、甲に生じた実際の損害額が同項に規定する損害賠償金の金額を超える場合において、甲がその超える分について乙に対し損害賠償金を請求することを妨げるものではない。
5　乙が、第 1 項の違約金及び前項の損害賠償金を甲が指定する期間内に支払わないときは、乙は、当該期間を経過した日から支払をする日までの日数に応じ、年 5 パーセントの割合で計算した金額の遅延利息を甲に支払わなければならない。

（暴力団関与の場合の契約の解除等）
第 4 条　甲は、乙（法人の場合にあっては、その役員又は使用人を含む。）について、暴力団員による不当な行為の防止等に関する法律（平成 3 年法律第 77 号）第 2 条に規定する暴力団又は暴力団員と関係があることが判明したときは、本契約を解除することができる。
2　乙が、本契約に関し、前項の規定に該当したときは、甲が本契約を解除するか否かにかかわらず、かつ、甲が損害の発生及び損害額を立証することを要することなく、乙は、契約金額（本契約締結後、契約金額の変更があった場合には、変更後の契約金額）の 100 分の 10 に相当する金額（その金額に 100 円未満の端数があるときは、その端数を切り捨てた金額）を違約金（損害賠償額の予定）として甲の指定する期間内に支払わなければならない。
3　前項の規定は、本契約による履行が完了した後も適用するものとする。
4　第 1 項に規定する場合において、乙が事業者団体であり、既に解散しているときは、甲は、乙の代表者であった者又は構成員であった者に違約金の支払を請求することができる。この場合において、乙の代表者であった者及び構成員であった者は、連帯して支払わなければならない。
5　第 2 項の規定は、甲に生じた実際の損害額が同項に規定する損害賠償金の金額を超える場合において、甲がその超える分について乙に対し損害賠償金を請求することを妨げるものではない。
6　乙が、第 2 項の違約金及び前項の損害賠償金を甲が指定する期間内に支払わないときは、乙は、当該期間を経過した日から支払をする日までの日数に応じ、年 5 パーセントの割合で計算した金額の遅延利息を甲に支払わなければならない。

上記合意を証するため本書面を 2 通作成し、甲乙記名押印の上各 1 通を保有する。

〇〇〇〇年〇月〇日

甲　東京都文京区本駒込二丁目 28 番 8 号
　　独立行政法人　情報処理推進機構
　　理事長　藤江 一正

乙　〇〇県〇〇市〇〇町〇〇丁目〇番〇号
　　株式会社〇〇〇〇
　　代表取締役　〇〇　〇〇　　印

様式 1

○○○○年○○月○○日

独立行政法人　情報処理推進機構
理事長あて

株式会社○○○○○○
代表取締役　○○　○○○

契約書第 2 条第 2 項に該当する件外プロダクトの利用承認について

○○○○年○○月○○日付け○○情財第○○○号「件名」に関する契約書第 2 条第 2 項の規定に該当する件外プロダクトの利用について承認申請いたします。

なお、当該件外プロダクトの利用に当たっては、同契約書第 9 条第 3 項（2）及び（3）並びに（4）を保証するとともに、納品時に同契約書第 6 条に基づく報告をいたします。

記

１．利用する件外プロダクトの名称
・○○○○○○○○エンジン（株式会社○○○○社製）
・○○○○○○○○ツール（株式会社○○○○社製）

２．件外プロダクト利用の内容

以上

様式 2

○○○○年○○月○○日

独立行政法人　情報処理推進機構
理事長あて

株式会社○○○○○○
代表取締役　○○　○○○

件外プロダクトリストの提出について

　○○○○年○○月○○日付け○○情財第○○○号「件名」に関する契約書第 6 条の規定に基づき、別紙のとおり件外プロダクトリストを提出いたします。

（様式 2：別紙 1）

件外プロダクトの一覧

契約番号
契約者
契約件名

通　番	件 外 プ ロ ダ ク ト の 名 称	承認対象

（様式 2：別紙 2）

件外プロダクトに関する記載

番号
件外プロダクトの名称

項目		記載内容	秘密性の有無
開発成果物に占める場所（または出現形態）			
開発成果物中への利用の方法と態様			
LPプロダクトの場合の記載項目	権利者の名称		
	権利者の連絡先		
	権利の内容		
	開発成果物への利用に付された条件の有無	条件有り　／　条件なし	
	上記条件の内容		
	第 2 条第 2 項の承認の対象か否か		
	上記承認の内容		
PDプロダクトの場合	ＰＤプロダクトの再入手の方法		
不分明の場合	知れたる関係者の名称		

＊別紙 1 リストに記載されたプロダクトそれぞれについて作成してください。

1. 開発成果物（第 1 条（1））

（1）中間納入物件

別添発注仕様書で定義された機能のうち、「GCM 及び GMAC」及び「XTS モード」の機能に関する部分を対象とする。

□以下記載の文書等を収めた記録媒体(CD-R 又は DVD-R)　　一式

① 暗号アルゴリズム実装試験ツール(JCATT)取扱説明書(日本語版及び英語版)

② 暗号アルゴリズム実装試験仕様書

③ JCATT ファイルフォーマット仕様書

④ ②③の生成に必要な LaTeX ソースファイル

⑤ テスト報告書、障害管理表(障害内容と対処内容の一覧表)

⑥ 設計資料(基本設計書、詳細設計書)

⑦ 納入物件一覧リスト及びソースコード一覧リスト

⑧ JCATT が入出力するファイルのサンプル

⑨ JCATT のソースコード及び実行形式生成に必要なファイル

⑩ JCATT の実行用ロードモジュール

（2）最終納入物件

別添発注仕様書で定義されたすべての機能を対象とする。

□以下記載の文書等を収めた記録媒体(CD-R 又は DVD-R)　　一式

① 暗号アルゴリズム実装試験ツール(JCATT)取扱説明書(日本語版及び英語版)

② 暗号アルゴリズム実装試験仕様書

③ JCATT ファイルフォーマット仕様書

④ ②③の生成に必要な LaTeX ソースファイル

⑤ テスト報告書、障害管理表(障害内容と対処内容の一覧表)

⑥ 設計資料(基本設計書、詳細設計書)

⑦ 納入物件一覧リスト及びソースコード一覧リスト

⑧ JCATT が入出力するファイルのサンプル

⑨ JCATT のソースコード及び実行形式生成に必要なファイル

⑩ JCATT の実行用ロードモジュール

⑪ JCATT 開発成果報告書及びその概要版

2. 原プロダクト（第 1 条（6））

JCATT バージョン 2.3.0

3. 納入（第 5 条第 1 項）

（1）納入期限

・中間納入期限　2011 年○月○日

・最終納入期限　2011 年○月○日

（2）納入場所

東京都文京区本駒込二丁目 28 番 8 号

独立行政法人　情報処理推進機構　セキュリティセンター

（3）納入による費用負担

乙の負担

4．対価の支払（第 10 条）

契約金額

金.〇〇，〇〇〇，〇〇〇円（うち消費税及び地方消費税額　金.〇，〇〇〇，〇〇〇円）

別紙 2

個人情報の取扱いに関する特則

（定　義）

第 1 条　本特則において、「個人情報」とは、請負業務に関する情報のうち、個人に関する情報であって、当該情報に含まれる記述、個人別に付された番号、記号その他の符号又は画像もしくは音声により当該個人を識別することのできるもの（当該情報のみでは識別できないが、他の情報と容易に照合することができ、それにより当該個人を識別できるものを含む。）をいい、秘密であるか否かを問わない。以下各条において、右「当該個人」を「情報主体」という。

（責任者の選任）

第 2 条　乙は、個人情報を取扱う場合において、個人情報の責任者を選任して甲に届け出る。

2　乙は、第 1 項により選任された責任者に変更がある場合は、直ちに甲に届け出る。

（個人情報の収集）

第 3 条　乙は、請負業務遂行のため自ら個人情報を収集するときは、「個人情報の保護に関する法律」その他の法令に従い、適切且つ公正な手段により収集するものとする。

（開示・提供の禁止）

第 4 条　乙は、個人情報の開示・提供の防止に必要な措置を講じるとともに、甲の事前の書面による承諾なしに、第三者（情報主体を含む）に開示又は提供してはならない。但し、法令又は強制力ある官署の命令に従う場合を除く。

2　乙は、請負業務に従事する従業員以外の者に、個人情報を取り扱わせてはならない。

3　乙は、請負業務に従事する従業員のうち個人情報を取り扱う従業員に対し、その在職中及びその退職後においても個人情報を他人に開示・提供しない旨の誓約書を提出させるとともに、随時の研修・注意喚起等を実施してこれを厳正に遵守させるものとする。

（目的外使用の禁止）

第 5 条　乙は、個人情報を請負業務遂行以外のいかなる目的にも使用してはならない。

（複写等の制限）

第 6 条　乙は、甲の事前の書面による承諾を得ることなしに、個人情報を複写又は複製してはならない。但し、請負業務遂行上必要最小限の範囲で行う複写又は複製については、この限りではない。

（個人情報の管理）

第 7 条　乙は、個人情報を取り扱うにあたり、本特則第 4 条所定の防止措置に加えて、個人情報に対する不正アクセスまたは個人情報の紛失、破壊、改ざん、漏えい等のリスクに対し、合理的な安全対策を講じなければならない。

2　乙は、前項に従って講じた措置を、遅滞なく甲に書面で報告するものとする。これを変更した場合も同様とする。

3　甲は、乙に事前に通知の上乙の事業所に立入り、乙における個人情報の管理状況を調査することができる。

4　前三項に関して甲が別途に管理方法を指示するときは、乙は、これに従わなければならない。

5　乙は、請負業務に関して保管する個人情報（甲から預託を受け、或いは乙自ら収集したものを含む）について甲から開示・提供を求められ、訂正・追加・削除を求められ、或いは請負業務への利用の停止を求められた場合、直ちに且つ無償で、これに従わなければならない。

（返還等）

第 8 条　乙は、甲から要請があったとき、又は請負業務が終了（本契約解除の場合を含む）したときは、個人情報が含まれるすべての物件（これを複写、複製したものを含む。）を直ちに甲に返還し、又は引き渡すとともに、乙のコンピュータ等に登録された個人情報のデータを消去して復元不可能な状態とし、その旨を甲に報告しなければならない。但し、甲から別途に指示があるときは、これに従うものとする。

2　乙は、甲の指示により個人情報が含まれる物件を廃棄するときは、個人情報が判別できないよう必要な処置を施した上で廃棄しなければならない。

（記録）

第 9 条　乙は、個人情報の受領、管理、使用、訂正、追加、削除、開示、提供、複製、返還、消去及び廃棄についての記録を作成し、甲から要求があった場合は、当該記録を提出し、必要な報告を行うものとする。

2　乙は、前項の記録を請負業務の終了後 5 年間保存しなければならない。

（再請負）

第 10 条　乙が甲の承諾を得て請負業務を第三者に再請負する場合は、十分な個人情報の保護水準を満たす再請負先を選定するとともに、当該再請負先との間で個人情報保護の観点から見て本特則と同等以上の内容の契約を締結しなければならない。この場合、乙は、甲から要求を受けたときは、当該契約書面の写しを甲に提出しなければならない。

2　前項の場合といえども、再請負先の行為を乙の行為とみなし、乙は、本特則に基づき乙が負担する義務を免れない。

（事　故）

第 11 条　乙において個人情報に対する不正アクセスまたは個人情報の紛失、破壊、改ざん、漏えい等の事故が発生したときは、当該事故の発生原因の如何にかかわらず、乙は、ただちにその旨を甲に報告し、甲の指示に従って、当該事故の拡大防止や収拾・解決のために直ちに応急措置を講じるものとする。なお、当該措置を講じた後ただちに当該事故及び応急措置の報告並びに事故再発防止策を書面により甲に提示しなければならない。

2　前項の事故が乙の本特則の違反に起因する場合において、甲が情報主体又は甲の顧客等から損害賠償請求その他の請求を受けたときは、甲は、乙に対し、その解決のために要した費用（弁護士費用を含むがこれに限定されない）を求償することができる。なお、当該求償権の行使は、甲の乙に対する損害賠償請求権の行使を妨げるものではない。

3　第 1 項の事故が乙の本特則の違反に起因する場合は、本契約第 16 条によって本契約が解除される場合を除き、乙は、前二項のほか、当該事故の善後策として必要な措置について、甲の別途の指示に従うものとする。

以上

独立行政法人　情報処理推進機構　入札心得
（総合評価落札方式）

（趣　旨）
第1条　当機構の契約に係る一般競争又は指名競争（以下「競争」という。）を行う場合において、入札者が知り、かつ遵守しなければならない事項は、法令に定めるもののほか、この心得に定めるものとする。

（仕様書等）
第2条　入札者は、仕様書、図面、契約書案及び添付書類を熟読のうえ入札しなければならない。
2　入札者は、前項の書類について疑義があるときは、関係職員に説明を求めることができる。
3　入札者は、入札後、第1項の書類についての不明を理由として異議を申し立てることができない。

（入札保証金及び契約保証金）
第3条　入札保証金及び契約保証金は、全額免除する。

（入札の方法）
第4条　入札者は、別紙様式による入札書を直接提出しなければならない。

（入札書の記載）
第5条　落札決定に当たっては、入札書に記載された金額に当該金額の5パーセントに相当する額を加算した金額をもって落札価格とするので、入札者は消費税に係る課税事業者であるか免税事業者であるかを問わず、見積もった契約金額の105分の100に相当する金額を入札書に記載すること。

（直接入札）
第6条　直接入札を行う場合は、入札書を封筒に入れ、封緘のうえ入札者の氏名を表記し、公告、公示又は通知書に示した時刻までに入札箱に投入しなければならない。この場合において、入札者に求められる義務を満たすことを証明する必要のある入札にあたっては、入札書とは別に証明書及び添付書類を契約担当官等に提出しなければならない。
2　入札者は、代理人をして入札させるときは、その委任状を持参させなければならない。

（代理人の制限）
第7条　入札者又はその代理人は、当該入札に対する他の代理をすることができない。
2　入札者は、予算決算及び会計令（昭和22年勅令第165号、以下「予決令」という。）第71条第1項各号の一に該当すると認められる者で、その事実があった後2年を経過しない者を入札代理人とすることができない。

（条件付きの入札）
第8条　予決令第72条第1項に規定する一般競争に係る資格審査の申請を行ったものは、競争に参加する者に必要な資格を有すると認められること又は指名競争の場合にあっては指名されることを条件に入札書を提出することができる。この場合において、当該資格審査申請書の審査が開札日までに終了しないとき又は資格を有すると認められなかったとき若しくは指名されなかったときは、当該入札書は落札の対象としない。

（入札のとりやめ等）
第9条　入札参加者が連合又は不穏の行動をなす場合において、入札を公正に執行することができないと認められるときは、当該入札者を入札に参加させず又は入札の執行を延期し、若しくはとりやめることがある。

（入札の無効）
第10条　次の各号の一に該当する入札は、無効とする。
（１）　競争に参加する資格を有しない者による入札

(２)　指名競争入札において、指名通知を受けていない者による入札
(３)　委任状を持参しない代理人による入札
(４)　記名押印（外国人又は外国法人にあっては、本人又は代表者の署名をもって代えることができる。）を欠く入札
(５)　金額を訂正した入札
(６)　誤字、脱字等により意思表示が不明瞭である入札
(７)　明らかに連合によると認められる入札
(８)　同一事項の入札について他人の代理人を兼ね又は2者以上の代理をした者の入札
(９)　入札者に求められる義務を満たすことを証明する必要のある入札にあっては、証明書が契約担当官等の審査の結果採用されなかった入札
(10)　入札書受領期限までに到着しない入札
(11)　その他入札に関する条件に違反した入札

（開　札）
第11条　開札には、入札者又は代理人を立ち会わせて行うものとする。ただし、入札者又は代理人が立会わない場合は、入札執行事務に関係のない職員を立会わせて行うものとする。

（調査基準価格、低入札価格調査制度）
第12条　工事その他の請負契約（予定価格が1千万円を超えるものに限る。）について予決令第85条に規定する相手方となるべき者の申込みに係る価格によっては、その者により当該契約の内容に適合した履行がされないこととなるおそれがあると認められる場合の基準は次の各号に定める契約の種類ごとに当該各号に定める額（以下「調査基準価格」という。）に満たない場合とする。
（1）工事の請負契約　その者の申込みに係る価格が契約ごとに3分の2から10分の8.5の範囲で契約担当官等の定める割合を予定価格に乗じて得た額
（2）前号以外の請負契約　その者の申込みに係る価格が10分の6を予定価格に乗じて得た額
2　調査基準価格に満たない価格をもって入札（以下「低入札」という。）した者は、事後の資料提出及び契約担当官等が指定した日時及び場所で実施するヒアリング等（以下「低入札価格調査」という。）に協力しなければならない。
3　低入札価格調査は、入札理由、入札価格の積算内訳、手持工事の状況、履行体制、国及び地方公共団体等における契約の履行状況等について実施する。

（落札者の決定）
第13条　契約担当官等が採用できると判断した提案書を入札書に添付して提出した入札者であって、その入札金額が予決令第79条の規定に基づいて作成された予定価格の制限の範囲内で、かつ提出した提案書と入札金額を当該入札説明書に添付の評価手順書に記載された方法で評価、計算し得た評価値が最も高かった者を落札者とする。
2　低入札となった場合は、一旦落札決定を保留し、低入札価格調査を実施の上、落札者を決定する。
3　前項の規定による調査の結果その者により当該契約の内容に適合した履行がされないおそれがあると認められるとき、又はその者と契約を締結することが公正な取引の秩序を乱すこととなるおそれがあって著しく不適当であると認められるときは、予定価格の制限の範囲内の価格をもって入札をした他の者のうち、評価の最も高い者を落札者とすることがある。

（再度入札）
第14条　開札をした場合において、各人の入札のうち予定価格の制限に達した価格の入札がないときは、直ちに再度の入札を行う。
　なお、開札の際に、入札者又はその代理人が立ち会わなかった場合は、再度入札を辞退したものとみなす。

（同総合評価点の入札者が2者以上ある場合の落札者の決定）
第15条　落札となるべき同総合評価点の入札をした者が2者以上あるときは、直ちに当該入札をした者又は第11条ただし書きにおいて立ち会いをした者にくじを引かせて落札者を決定する。
2　前項の場合において、当該入札をした者のうちくじを引かない者があるときは、これに代わって入札事務に関係のない職員にくじを引かせるものとする。

（契約書の提出）
第16条　落札者は、契約担当官等から交付された契約書に記名押印（外国人又は外国法人が落札者である場合には、本人又は代表者が署名することをもって代えることができる。）し、落札決定の日から5日以内（期終了の日が行政機関の休日に関する法律（昭和63年法律第91号）第1条に規定する日に当たるときはこれを算入しない。）に契約担当官等に提出しなければならない。ただし、契約担当官等が必要と認めた場合は、この期間を延長することができる。
2　落札者が前項に規定する期間内に契約書を提出しないときは、落札は、その効力を失う。

（入札書等に使用する言語及び通貨）
第17条　入札書及びそれに添付する仕様書等に使用する言語は、日本語とし、通貨は日本国通貨に限る。

（落札決定の取消し）
第18条　落札決定後であっても、この入札に関して連合その他の事由により正当な入札でないことが判明したときは、落札決定を取消すことができる。

以上

（参　考）

予算決算及び会計令【抜粋】

（一般競争に参加させることができない者）

第 70 条　契約担当官等は、売買、貸借、請負その他の契約につき会計法第二十九条の三第一項の競争（以下「一般競争」という。）に付するときは、特別の理由がある場合を除くほか、当該契約を締結する能力を有しない者及び破産者で復権を得ない者を参加させることができない。

（一般競争に参加させないことができる者）

第 71 条　契約担当官等は、一般競争に参加しようとする者が次の各号のいずれかに該当すると認められるときは、その者について三年以内の期間を定めて一般競争に参加させないことができる。その者を代理人、支配人その他の使用人として使用する者についても、また同様とする。

一　契約の履行に当たり故意に工事若しくは製造を粗雑にし、又は物件の品質若しくは数量に関して不正の行為をしたとき。

二　公正な競争の執行を妨げたとき又は公正な価格を害し若しくは不正の利益を得るために連合したとき。

三　落札者が契約を結ぶこと又は契約者が契約を履行することを妨げたとき。

四　監督又は検査の実施に当たり職員の職務の執行を妨げたとき。

五　正当な理由がなくて契約を履行しなかつたとき。

六　この項（この号を除く。）の規定により一般競争に参加できないこととされている者を契約の締結又は契約の履行に当たり、代理人、支配人その他の使用人として使用したとき。

2　契約担当官等は、前項の規定に該当する者を入札代理人として使用する者を一般競争に参加させないことができる。

III. 仕様書

「暗号アルゴリズム実装試験ツールの機能追加 (GCM/XTS/鍵確立手法)」

開発業務内容（発注仕様書）

独立行政法人 **情報処理推進機構**

開発業務内容（仕様書）

1. 件名

「暗号アルゴリズム実装試験ツールの機能追加(GCM/XTS/鍵確立手法)」

2. 背景・目的

2.1. 背景

独立行政法人 情報処理推進機構(以下「IPA」という。)では、「安心」して利用できる IT 基盤の構築・維持のため、情報セキュリティ対策の強化、整備を進めている。その一環として IPA では、暗号モジュールの適切な実装を確認するための、暗号モジュール試験及び認証制度(以下「JCMVP」という。)の正式運用を 2007 年 4 月から開始した。
JCMVP では、暗号モジュール試験に先立ち昨年度までに開発したツール(以下「JCATT」という。)を用いて暗号アルゴリズム実装試験を実施している。

2.2. 目的

北米の暗号モジュール認証制度(CMVP[1])において承認された暗号アルゴリズムにGalois/Counter Modeモード(GCM)及びXTSモードが追加されたこと、また、JCMVPにおいて承認された暗号アルゴリズムにNIST SP800-56Aに基づく鍵確立手法が追加されたことを受け、JCATTに同等以上の試験機能を追加することを本開発の目的とする。

3. 現行システム

3.1. 入出力ファイル及び運用方法の概略

3.1.1. 入出力ファイル

JCATT は、その運用に際して、以下のテキストファイルを入出力する。

(1) パラメータファイル(ファイルの拡張子は、par)
JCATT が生成するファイル。ベンダから依頼を受けた暗号アルゴリズム確認の試験条件が記録されている。

(2) 質問ファイル(ファイルの拡張子は、req)
JCATT が生成するファイル。暗号アルゴリズムに対する入力データ及び制御情報が記録されている。暗号モジュール試験機関からベンダ側へ送る。

(3) 正解ファイル(ファイルの拡張子は、fax)
JCATT が質問ファイルと同時に生成するファイル。暗号アルゴリズムに対する入力データ、制御情報及び対応する出力データが記録されている。暗号モジュール試験機関で保存し、回答ファイルが送られてきた際に回答ファイルと比較する。

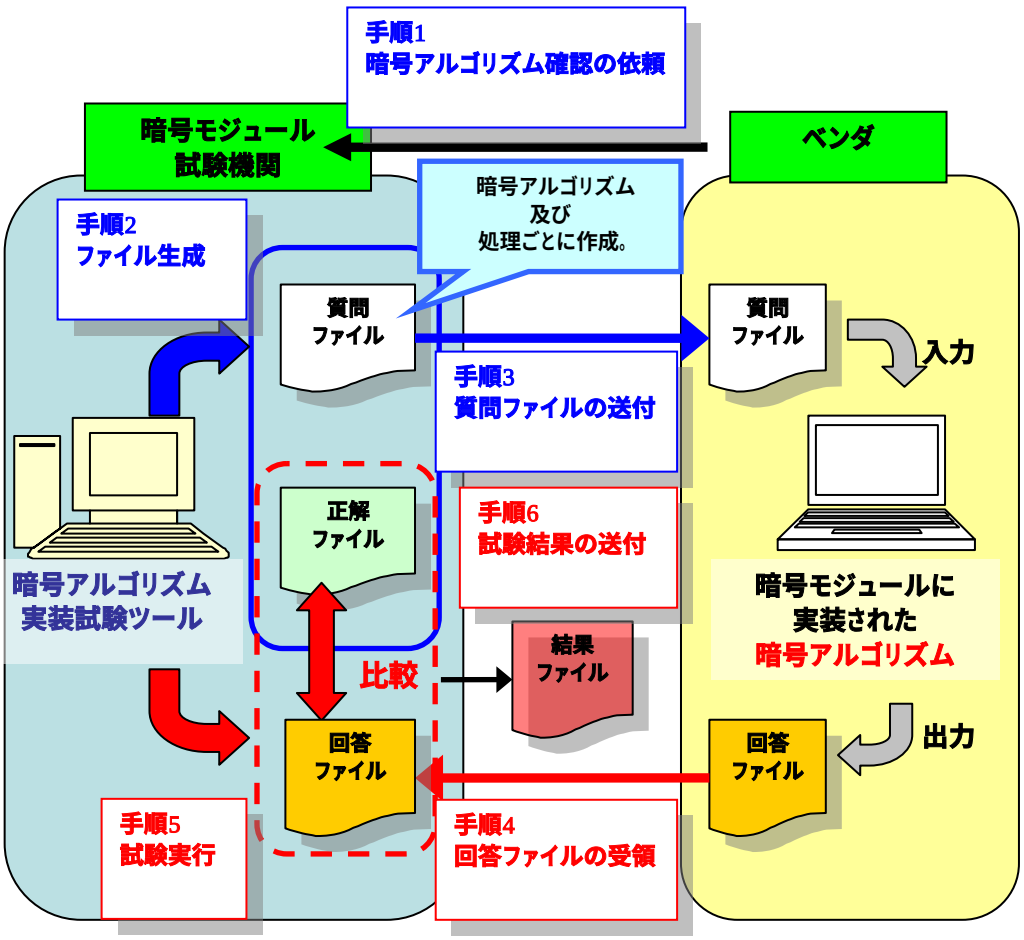
(4) 回答ファイル(ファイルの拡張子は、rsp)
ベンダ側で、質問ファイルを元に暗号モジュール(以下「IUT」という)が生成したテキストファイル。ベンダから暗号モジュール試験機関側へ送る。

(5) 結果ファイル(ファイルの拡張子は、out)
回答ファイルの内容を正解ファイルの内容と照らし合わせて、結果(正解又は不正解)を出力するファイル。

3.1.2. JCATT の運用方法

JCATT の運用方法の概略を下図に示す。

[1] http://csrc.nist.gov/groups/STM/cmvp/index.html



この運用方法を文書化すると、以下のようになる。

- 手順 1: 暗号アルゴリズム確認の依頼
  暗号モジュール試験機関は、ベンダから暗号アルゴリズム確認の依頼を受け付ける。このとき、試験対象の暗号アルゴリズムと試験条件についての情報をベンダから受領する。
- 手順 2: ファイル生成
  試験対象の暗号アルゴリズムを選択し、手順 1.で受領した試験条件を入力して、まず、パラメータファイルを作成する。JCATT のファイル生成機能を使用して、パラメータファイルに記録された試験条件に基づく質問ファイル及び正解ファイルを作成する。
- 手順 3: 質問ファイルの送付
  手順 2 で生成した質問ファイルをベンダに送付する。
- 手順 4: 回答ファイルの受領
  手順 3.で送付した質問ファイルに対する回答ファイルをベンダから受領する。
- 手順 5: 試験実行
  手順 4 で受領した回答ファイルと手順 2.で生成した正解ファイルを比較することにより、暗号アルゴリズム実装試験を実行する。合格及び不合格といった試験結果は、結果ファイルに記録される。
- 手順 6: 試験結果の送付
  手順 5 で生成された結果ファイルをベンダに送付する。

3.2. JCATT の構成

3.2.1. JCATT の構成ファイル

現状の JCATT を構成するファイルの内、今回の開発に関連するファイルを表 1に示す。

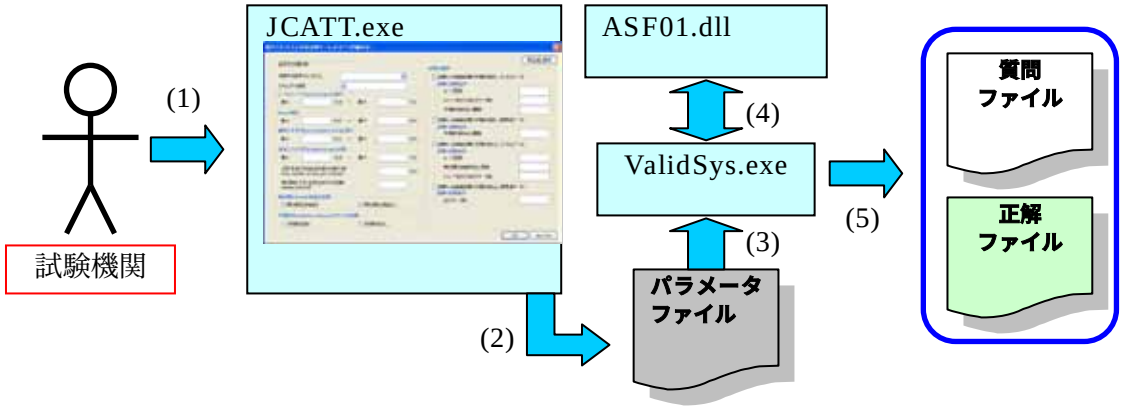
表1 JCATT の構成ファイル

利用者	ファイル名	概要
IPA	SetupTool.exe	JCATTをインストールする環境のMACアドレス(Media Access Control Address)を入力として、暗号アルゴリズムである AES-CBC-MAC を用いた認証データファイル(JCATT_MAC.txt)を生成するプログラム。 【今回の機能追加開発対象】
暗号モジュール試験機関(IPAを含む)	JCATT.exe	GUI プログラム。 画面から入力された試験条件を元に、パラメータファイルを生成する。 【今回の機能追加開発対象】
	ValidSys.exe	JCATT.exe から起動されるバックエンド・プログラム。 通常、ユーザによって明示的に起動されることはない。 以下の 2 つの機能を有する: 1. パラメータファイルを元に、質問ファイル及び正解ファイルを生成する。 2. 回答ファイルと正解ファイルを比較し、合格又は不合格を判定する。 【今回の機能追加開発対象】
	JCATT.ini	JCATT.exe の動作設定を記述するテキストファイル。ユーザインタフェースの表示言語(日本語/英語)の切り替え、試験対象機能選択画面においての、デフォルトでのチェックボックスの選択状態の設定に、主に使用される。 【今回の改修対象】
	JCATT_MAC.txt	JCATT の完全性のチェックのために使用されるファイル。前述の SetupTool.exe を用いて IPA で生成される。
	CryptoAlgorithms.dll	以下の暗号アルゴリズムを実装する動的リンクライブラリ。 ü AES-CBC-MAC ü ANSI X9.42 KDF with SHA-1 based on Concatenation SetupTool.exe 及び JCATT.exe から呼出され、試験ツールの完全性、不正改造検出機能に使用される。
	ASF01.dll	今回開発対象の以下の暗号アルゴリズムを実装する。 ü Galois/Counter Mode(GCM)/GMAC ü XTS モード ü 鍵確立手法 【今回の機能追加開発対象】
	HC3.dll HCL1.dll unie.dll unia128.dll unia192.dll unia256.dll DLL_CIPHERUNICORNA128.dll DLL_CIPHERUNICORNA192.dll DLL_CIPHERUNICORNA256.dll DLL_CIPHERUNICORNE.dll DLL_Hierocrypto.dll DLL_HIME.dll DLL_MUGI.dll DLL_MULTIS01.dll DLL_PSEC.dll DLL_SC2000.dll DLL_DRBG.dll	電子政府推奨暗号リストに記載された暗号アルゴリズムを実装した動的リンクライブラリ。 今回の改修対象ではない。

3.2.2. JCATT の構成ファイルとデータの流れ

3.2.2.1. 質問ファイル及び正解ファイル生成時

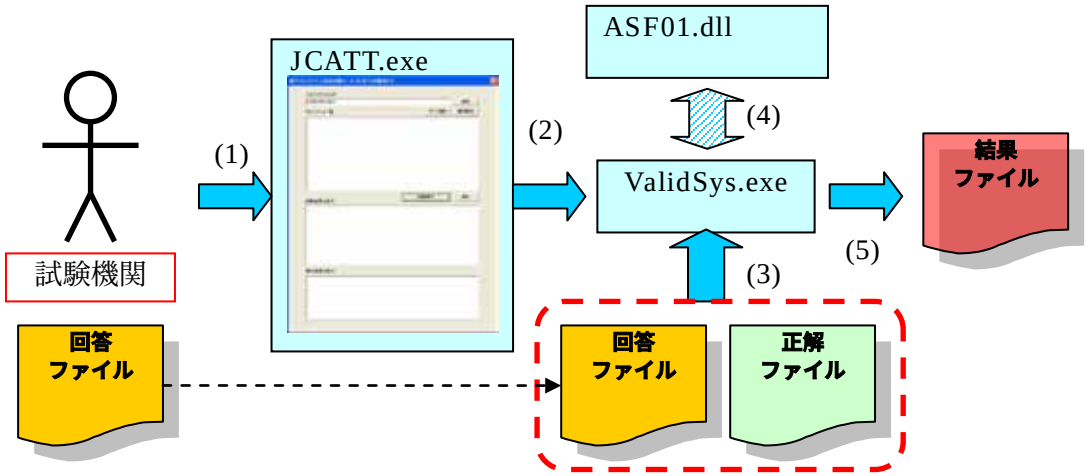
3.1.2 手順 2.のデータの流れを図示したものが、下の図である。



図中の(1)～(5)の説明は、以下の通りである。
(1)画面から試験条件を入力する。
(2)画面から入力された試験条件をパラメータファイルに出力する。
(3)ValidSys.exe がパラメータファイルに記載された試験条件を読み込む。
(4)試験条件を元に、試験パターンに基づく入力データを ASF01.dll を用いて生成する。
(5)(4)の試験パターンに基づく質問ファイル及び正解ファイルを出力する。

3.2.2.2. 試験実行時

3.1.2 手順 5.のデータの流れを図示したものが、下の図である。



図中の(1)～(5)の説明は、以下の通りである。
(1)回答ファイルを入力すると共に、画面から試験を実行する。
(2)試験を実行する回答ファイル及び対応する正解ファイルを ValidSys.exe に指定する。
(3)指定された回答ファイル及び対応する正解ファイルを読み込む。
(4)試験パターンが既知解テストでない場合、回答ファイルに記載された暗号アルゴリズムの入力データを ASF01.dll に入力して、回答ファイルに記載された暗号アルゴリズムの出力データが再現できるか検証を行う。
(5)試験パターンが既知解テストの場合、回答ファイル及び正解ファイルを比較し、試験結果を結果ファイルに出力する。試験パターンが既知解テストでない場合、(4)で行った検証結果を結果ファイルに出力する。

4. 開発内容

4.1. 開発項目概要

今回の開発項目は以下の 7 項目である。以下の 7 項目の詳細については、「5. 開発機能詳細」および「6.ドキュメント」で記述する。

(1) 暗号アルゴリズムの実装
- Galois/Counter Mode (GCM) 及び GMAC
- XTS モード
- NIST SP800-56A に記載された鍵確立スキーム

(2) 暗号アルゴリズムの試験機能の実装
- Galois/Counter Mode (GCM) 及び GMAC
- XTS モード
- NIST SP800-56A に記載された鍵確立スキーム

(3) 暗号アルゴリズムの試験機能追加に伴う GUI の改修
(4) 試験ツールの完全性、不正改造検出機能
(5) 取扱説明書の作成
(6) JCATT ファイルフォーマット仕様書の作成
(7) 暗号アルゴリズム実装試験仕様書の作成
(8) JCATT が入出力するファイルのサンプルの作成

なお、本仕様書では、以下 Galois/Counter Mode を単に GCM と表記する。GMAC に関しては、GCM と独立した API(Application Program Interface)を提供せず、GCM において暗号文/平文の長さに 0 を指定させるという方式としてもよい。

また、プログラム及びドキュメントは、公開を前提とした整備を行うこと。

4.2. JCATT の動作環境

開発する JCATT の動作環境は次の通りとする。
- OS：以下のいずれでも動作すること
  - Microsoft Windows XP Professional SP3
    (32 ビット環境、日本語及び英語版)
  - Microsoft Windows 7 Professional
    (32 ビット環境及び 64 ビット環境、日本語及び英語版)
- CPU：Intel Pentium 4 プロセッサまたはその同等品
- RAM：1024MB 以上

4.3. JCATT の開発環境

JCATT の開発には Microsoft Visual C++ 2005 + SP1 あるいは Microsoft Visual Studio2010 を使用し、C/C++言語で実装すること。ドキュメントとソースコードは構成管理ツールを使用して適切なバージョン管理を行うこと。
また、試験は Visual Studio のためのテスト方法論(以下の URL 参照)
http://www.microsoft.com/japan/msdn/architecture/TestingMethodologyForVSTS/
又は、単体テスト用のフレームワーク CppUnit(以下の URL 参照)
http://sourceforge.net/projects/cppunit/
あるいは開発会社で規定されている開発・試験手順に基づいて、単体テスト、結合テスト、システムテストを実施すること。

5. 開発機能詳細

5.1. 暗号アルゴリズムの実装

5.1.1. GCM 及び GMAC

NIST SP800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*
(http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf)の Section 7 に記載されている認証暗号化及び復号検証のアルゴリズムを実装すること。

ただし、組み合わせる 128-bit ブロック暗号アルゴリズムは、AES[2]に限らず、JCMVPで承認されたすべての 128-bitブロック暗号アルゴリズム[3] (AES, Camellia, CIPHERUNICORN-A, Hierocrypt-3, SC2000)とすること。

5.1.2. XTS モード

NIST SP800-38E, *Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices*
(http://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf)の Section 4 に基づいて暗号化及び復号のアルゴリズムを実装すること。

ただし、組み合わせる 128-bit ブロック暗号アルゴリズムは、AES に限らず、JCMVP で承認されたすべての 128-bit ブロック暗号アルゴリズム(AES, Camellia, CIPHERUNICORN-A, Hierocrypt-3, SC2000)とすること。

5.1.3. NIST SP800-56A に記載された鍵確立スキーム

NIST SP800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)*
(http://csrc.nist.gov/publications/nistpubs/800-56A/SP800-56A_Revision1_Mar08-2007.pdf)に記載されている鍵確立スキームのうち、表 2で「開発対象」が「○」になっている 5 個のスキームを実装すること。

表 2 鍵確立スキーム一覧

プリミティブ	スキーム	開発対象
FFC DH	dhHybrid1	○
	dhEphem	○
	dhHybridOneFlow	○
	dhOneFlow	○
	dhStatic	○
ECC CDH	Full Unified Model	
	Ephemeral Unified Model	
	One-Pass Unified Model	
	One-Pass Diffie-Hellman	
	Static Unified Model	
FFC MQV	MQV2	
	MQV1	
ECC MQV	Full MQV	
	One-Pass MQV	

[2] Advanced Encryption Standard
[3] JCMVP で承認された 128 ビットブロック暗号アルゴリズムに関しては、
http://www.ipa.go.jp/security/jcmvp/algorithm.html を参照

また、開発対象のスキームのうち dhEphem を除くものについては、NIST SP800-56A の Section 8 に記載されている Key Confirmation を実装すること。
Key Confirmation で使用するメッセージ認証子(MAC)アルゴリズムは、CCM、CMAC、HMAC とすること。

5.1.4. 実装にあたっての補足説明

現行の JCATT では既に多倍長整数演算ライブラリとして GnuMP (http://gmplib.org/)を使用しているため、多倍長整数演算機能を新規開発する必要はない。
また、経済産業省による「新世代情報セキュリティ研究開発事業 (クラウドコンピューティングセキュリティ技術開発)」において、暗号プリミティブを開発した(公募仕様書 (http://www.meti.go.jp/information/data/c90710bj.html) 参照)の 3.2 クラウド環境における暗号技術評価 参照)。この事業の成果物には、GCM、GF(2^m)の演算機能、楕円曲線演算(点の加算、2 倍、スカラー倍)、ECC KAS の機能がソースコードも込みで含まれており、IPA が JCATT に組み込むためにその成果物を利用することが可能であるため、本開発においてはこれらの暗号プリミティブの新規開発は不要である。ただし、この成果物は本開発を行う者に対して開示をするが、一般公開されないソフトウェアを含むため、秘密情報として扱い、秘密保持を行うこと。

5.2. 暗号アルゴリズムの試験機能の実装

5.2.1. GCM 及び GMAC

GCM 及び GMAC の試験対象機能は次のとおり。

- 暗号化機能
- 復号機能

AES に限らず、JCMVP で承認されたすべての 128-bit ブロック暗号アルゴリズムとの組み合わせを試験できるようにすること。

5.2.1.1. 暗号化機能試験

暗号化機能試験については、IV(Initial Vector)が外部で生成されるか、内部で生成されるかに応じた試験を行う。

- 外部生成 IV に対する試験
  IUT が IV を外部から取り込む場合、複数個(別途指定する値) のランダムな鍵、平文、AAD(Additional Autheticated Data)、IV を与える。IUT はそれらの値から暗号文及び Authentication Tag を出力する。
  JCATT は、IUT から出力された暗号文及び Authentication Tag が期待値と一致するかどうかを試験する。
  鍵長、平文長、AAD 長、IV 長は別途定める規定値とする。

- 内部生成 IV に対する試験
  IUT が IV を内部で生成する場合、複数個(別途指定する値)のランダムな鍵、平文、AAD(Additional Autheticated Data) を与える。IUT は内部で IV を生成し、その IV を、暗号文及び Authentication Tag とともに出力する。JCATT は、IUT が出力した暗号文及び Authentication Tag が、AAD、IUT の内部で生成された IV から生成される正しい暗号文、Authentication Tag と一致するかどうかを試験する。
  IUT が以下の条件を満たしたとき、試験は合格とする。
  - Ø 与えられた暗号文、鍵、AAD に対して、もとの平文に復号できること。
  - Ø 復号機能で INVALID 出力となるような、暗号文、鍵、AAD、の組に対して、INVALID

を出力すること
鍵長、平文長、AAD 長、IV 長は別途定める規定値とする。

5.2.1.2. 復号機能試験

JCATT は複数個(別途指定する値) のランダムな鍵、平文、AAD から暗号文、Authentication Tag を生成する。それらのデータのうちのいくつかを改ざんし、検証がエラーとなるようにする。改ざんは暗号文あるいは Authentication Tag に対して行う。
IUT が以下の条件を満たしたとき、試験は合格とする。

- 与えられた暗号文、Authentication Tag、鍵、AAD、IV に対して、もとの平文に復号できること。
- 復号機能では INVALID 出力となるような、暗号文、Authentication Tag、鍵、AAD、IV の組に対して、INVALID を出力すること。

鍵長、平文長、AAD 長、IV 長、改ざんするデータの割合は別途定める規定値とする。

5.2.2. XTS モード

XTS モードの試験対象機能は次のとおり。

- 暗号化機能
- 復号機能

AES に限らず、すべての承認された 128-bit ブロック暗号アルゴリズムとの組み合わせを試験できるようにすること。

5.2.2.1. 暗号化機能試験

入力データ(平文、暗号鍵及び tweak)を様々に変化させ、暗号文が期待値と一致するかどうかを試験する。入力データの組の数は、別途定める規定値とする。

5.2.2.2. 復号機能試験

入力データ(暗号文、暗号鍵及び tweak) を様々に変化させ、平文が期待値と一致するかどうかを試験する。入力データの組の数は、別途定める規定値とする。

5.2.3. NIST SP800-56A に記載された鍵確立スキーム

5.2.3.1. Diffie-Hellman (DH) 鍵確立スキーム

JCMVP では、NIST SP800-56A に記述されている FFC DH 鍵確立スキームのうち、以下の 5 個のスキームを承認している。

- dhHybrid1
- dhEphem
- dhHybridOneFlow
- dhOneFlow
- dhStatic

これらの 5 個のスキームに関する試験機能を実装する。試験対象機能は、各スキーム共に次のとおり。

- ドメインパラメータ生成機能
- ドメインパラメータ検証機能

- 鍵ペア生成機能
- 公開鍵検証機能
- 鍵共有機能

5.2.3.1.1. ドメインパラメータ生成機能試験

ドメインパラメータ生成機能試験の試験項目は次の通りである。
ドメインパラメータのうち p と q については、

- FIPS 186-3 Appendix A 1.1.2 “Generation of the FFC Primes p and q Using an Approved Hash Function”

に記述されているドメインパラメータ生成法に従って p と q が生成されていることを試験する。
また、ドメインパラメータ g については、

- FIPS 186-3 Appendix A 2.1 “Unverifiable Generation of the Generator g”
- FIPS 186-3 Appendix A 2.3 “Verifiable Generation of the Generator g”

に記述されているドメインパラメータ生成法に従って g が生成されていることを試験する。

5.2.3.1.1.1. 試験 1 (Testing on FIPS 186-3 A.2.1 Unverifiable Generation of the Generator g (既定の試験))

- IUT が生成した *SEED* および *counter* を JCATT に入力し、JCATT は FIPS 186-3 Appendix A 1.1.2 のアルゴリズムに従って 2 つの素数 p', q' を計算する。この p', q' と、IUT が生成した p, q がそれぞれ等しいこと。
- $2 \leq g \leq p-1$ であること。
- $g^p \equiv 1 \bmod p$ であること。
- IUT が生成した複数(別途指定する数)のドメインパラメータ *(p, q, g)* がすべて異なるものであること。

5.2.3.1.1.2. 試験 2 (Testing on FIPS 186-3 A.2.3 Verifiable Generation of the Generator g)

- IUT が生成した *SEED* および *counter* を JCATT に入力し、JCATT は FIPS 186-3 Appendix A 1.1.2 のアルゴリズムに従って 2 つの素数 p', q' を計算する。この p', q' と、IUT が生成した p, q がそれぞれ等しいこと。
- IUT が生成した *SEED* および *counter* を JCATT に入力し、JCATT は FIPS 186-3 Appendix A 2.3 のアルゴリズムに従って g' を計算する。この g' と、IUT が生成した g, q が等しいこと。
- IUT が生成した複数(別途指定する数)のドメインパラメータ *(p, q, g)* がすべて異なるものであること。

なおドメインパラメータ生成において使用するハッシュ関数は、FIPS186-3 に従って次の通りとする($|p|$ を p のビット長、$|q|$ を q のビット長とする)。

- $|p| = 1024, |q| = 160$ ... SHA-1
- $|p| = 2048, |q| = 224$ ... SHA-224
- $|p| = 2048, |q| = 256$ ... SHA-256

また、FIPS 186-3 Appendix A 1.2 に記載された Shawe-Taylor アルゴリズムを用いたドメインパラメータ生成機能に対する試験は行わない。

5.2.3.1.2. ドメインパラメータ検証機能試験

ドメインパラメータ検証機能試験の試験項目は次の通りである。

5.2.3.1.2.1. 試験 1 (Testing on FIPS 186-3 A.2.2 Assurance of the Validity of the Generator g (既定の試験))

- JCATT が与えた前節試験 1 に記述したドメインパラメータ生成機能に対する試験に適合するようなドメインパラメータに対して、IUT が”合格”と判定すること。
- JCATT が与えた前節試験 1 に記述したドメインパラメータ生成機能に対する試験に違反するようなドメインパラメータに対して、IUT が”不正”と判定すること。

5.2.3.1.2.2. 試験 2 (Testing on FIPS 186-3 A.2.4 Validation Routine when the Canonical Generation of the Generator g RoutineWas Used)

- JCATT が与えた前節試験 2 に記述したドメインパラメータ生成機能に対する試験に適合するようなドメインパラメータに対して、IUT が”合格”と判定すること。
- JCATT が与えた前節試験 2 に記述したドメインパラメータ生成機能に対する試験に違反するようなドメインパラメータに対して、IUT が”不正”と判定すること。

前節に記述したように、p と q については FIPS 186-3 Appendix A 1.1 に基づくドメインパラメータ検証機能を試験の対象とし、FIPS 186-3 Appendix A 1.2 に基づくドメインパラメータ検証機能に対しては試験を行わない。

5.2.3.1.3. 鍵ペア生成機能試験

既存の Diffie-Hellman(DH)に対する公開鍵検証機能試験を NIST SP800-56A に記載された Diffie-Hellman(DH)に対して実装すること。

5.2.3.1.4. 公開鍵検証機能試験

既存の Diffie-Hellman(DH)に対する公開鍵検証機能試験を NIST SP800-56A に記載された Diffie-Hellman(DH)に対して実装すること。

5.2.3.1.5. 鍵共有機能試験

NIST SP800-56A に記載された鍵共有機能の試験は、以下に挙げる、アルゴリズムがサポートするオプションに応じて、試験項目が異なる。

- Key Confirmation のサポートの有無
  → 試験 1
- Key Confirmation をサポートする場合、Key Confirmation の種別
  - Ø Unilateral
    → 試験 2
    - IUT が Key Confirmation Provider の場合
    - IUT が Key Confirmation Recipient の場合
  - Ø Bilateral
    → 試験 3

試験 1～試験 3 で使用可能な鍵導出関数(Key Derivation Function : KDF)は、NIST SP800-56A に記載された次の KDF を使用可能とすること。

- SHA-1 を用いた Concatenation に基づく KDF
- SHA-224 を用いた Concatenation に基づく KDF
- SHA-256 を用いた Concatenation に基づく KDF

- SHA-384 を用いた Concatenation に基づく KDF
- SHA-512 を用いた Concatenation に基づく KDF
- SHA-1 を用いた ASN.1 に基づく KDF
- SHA-224 を用いた ASN.1 に基づく KDF
- SHA-256 を用いた ASN.1 に基づく KDF
- SHA-384 を用いた ASN.1 に基づく KDF
- SHA-512 を用いた ASN.1 に基づく KDF

また、試験 2、試験 3 で使用可能なメッセージ認証子(MAC)アルゴリズムは、CCM、CMAC、HMAC とすること。

5.2.3.1.5.1. 試験 1

- JCATT が与えた OtherInfo の構成要素、5.2.3.1.4に記述した公開鍵検証試験に適合するようなドメインパラメータ、公開鍵に対して、IUT が正しい *DerivedKeyingMaterial* (DKM) を生成すること。
- 正しい DKM が生成されたかどうかの検証は、次の何れかの検証方法によって行う。
  - DKM を直接検証
  - NIST SP800-56A の 5.2.3 に記載の方法で計算する *MacTag* の検証
- IUT が生成した複数(別途規定する数) の共有鍵がすべて異なるものであること。
- JCATT が与えた OtherInfo の構成要素、5.2.3.1.4に記述した公開鍵検証試験に違反するようなドメインパラメータ、公開鍵に対して、IUT がエラーを出力すること。

5.2.3.1.5.2. 試験 2

5.2.3.1.5.2.1. Key Confirmation Provider の場合

JCATT が与えた正しいドメインパラメータ、公開鍵、プライベート鍵、OtherInfo の構成要素、*MacData*、該当する場合には *Nonce* に対して、IUT が正しい *KeyData* 及び *MacTag* を生成すること。

5.2.3.1.5.2.2. Key Confirmation Recipient の場合

- JCATT が与えた正しいドメインパラメータ、公開鍵、プライベート鍵、OtherInfo の構成要素、*MacData*、*MacTag*、該当する場合には *Nonce* に対して、IUT が正しい *KeyData* を生成し、*MacTag* を検証合格と判定すること。
- JCATT が与えた改ざんされたドメインパラメータ、公開鍵、プライベート鍵、OtherInfo の構成要素、*MacData*、*MacTag*、該当する場合には *Nonce* に対して、IUT がエラーを出力するか又は *MacTag* を検証不合格と判定すること。

5.2.3.1.5.3. 試験 3

- JCATT が与えた正しいドメインパラメータ、公開鍵、プライベート鍵、OtherInfo の構成要素、Key Confirmation Provider の *MacTag*、該当する場合には *Nonce* に対して、IUT が正しい *KeyData* 及び Key Confirmation Recipient の *MacTag* を生成し、Key ConfirmationProvider の *MacTag* を検証合格と判定すること。
- JCATT が与えた改ざんされたドメインパラメータ、公開鍵、プライベート鍵、OtherInfo の構成要素、Key Confirmation Provider の *MacTag*、該当する場合には *Nonce* に対して、IUT がエラーを出力するか又は Key Confirmation Provider の *MacTag* を検証不合格と判定すること。

5.2.3.2. Elliptic Curve Cryptography Cofactor Diffie-Hellman (ECC CDH) 鍵確立スキーム

JCMVP では、NIST SP800-56A に記述されている ECC CDH 鍵確立スキームの内、Ephemeral Unified Model のみを承認しているため Ephemeral Unified Model に対する試験機能のみを実装する。

Ephemeral Unified Model の試験対象機能は次のとおり。

- ドメインパラメータ生成機能
- ドメインパラメータ検証機能
- 鍵ペア生成機能
- 公開鍵検証機能
- 鍵共有機能

5.2.3.2.1. ドメインパラメータ生成機能試験

標数 p の場合

- セキュリティレベルを s として、n が $\max(2^{2s-1},160)$ ビット以上であること。
- $4a^3+27b^2 \neq 0 \pmod p$ であること。
- a, b, x_G, y_G が 0 以上 $p-1$ 以下の整数であること。
- $y_G^2 \equiv x_G^3 + ax_G + b \pmod p$ であること。
- n が素数であること。
- p が素数であること。
- $h \leq 2^{s/8}$ かつ $h = \lfloor(\sqrt{p}+1)^2/n\rfloor$ であること。
- $nG = O$ であること。
- すべての $1 \leq B < 100$ に対して $p^B \neq 1 \pmod n$ であること。
- $nh \neq p$ であること。
- ANS X9.62-2005 の A.3.2.2 に記載された Anomalous condition が成立すること。
- IUT が生成した複数(別途規定する数) のドメインパラメータがすべて異なるものであること。

標数 2 の場合

- セキュリティレベルを s として、n が $\max(2^{2s-1},160)$ ビット以上であること。
- $f(x)$が次数 m の F_2 上既約多項式であること。
- a, b, x_G, y_G が次数 m-1 以下の F_2 上多項式であること。
- $b \neq 0$ in F_{2^m} であること。
- $y_G^2 + x_G y_G = x_G^3 + ax_G^2 + b$ in F_{2^m} であること。
- n が素数であること。
- $h \leq 2^{s/8}$ かつ $h = \lfloor(\sqrt{2^m}+1)^2/n\rfloor$ であること。
- $nG = O$ であること.
- すべての $1 \leq B < 100$ に対して $2^{mB} \neq 1 \pmod n$ であること。
- $nh \neq 2^m$ であること。
- ANS X9.62-2005 の A.3.2.2 に記載された Anomalous condition が成立すること。
- IUT が生成した複数(別途規定する数) のドメインパラメータがすべて異なるものであること。

5.2.3.2.2. ドメインパラメータ検証機能試験

- JCATT が与えた前節に記述したドメインパラメータ生成機能試験項目に適合するよう

なドメインパラメータに対して、IUT が“合格”と判定すること。
- JCATT が与えた前節に記述したドメインパラメータ生成機能試験項目に違反するようなドメインパラメータに対して、IUT が“不正”と判定すること。

5.2.3.2.3. 鍵ペア生成機能試験

既存の ECDH に対する鍵ペア生成機能試験を NIST SP800-56A に記載された ECC CDH に対して実装すること。

5.2.3.2.4. 公開鍵検証機能試験

既存の ECDH に対する公開鍵検証機能試験を NIST SP800-56A に記載された ECC CDH に対して実装すること。

5.2.3.2.5. 鍵共有機能試験

- JCATT が与えた OtherInfo の構成要素、5.2.3.2.4に記述した公開鍵検証試験に適合するようなドメインパラメータ、公開鍵に対して、IUT が正しい *DerivedKeyingMaterial*(DKM) を生成すること。
- 正しい DKM が生成されたかどうかの検証は、次の何れかの検証方法によって行う。
  - DKM を直接検証
  - NIST SP800-56A の 5.2.3 に記載の方法で計算する *MacTag* の検証
- IUT が生成した複数(別途規定する数) の共有鍵がすべて異なるものであること。
- JCATT が与えた OtherInfo の構成要素、5.2.3.2.4に記述した公開鍵検証試験に違反するようなドメインパラメータ、公開鍵に対して、IUT がエラーを出力すること。

5.3. 暗号アルゴリズムの試験機能追加に対応する GUI の改修
5.3.1. JCATT の画面構成

5.3.1.1. 起動から暗号アルゴリズム選択画面まで

今回機能追加開発する JCATT について、その起動時から、暗号アルゴリズム選択画面までの画面遷移を以下に示す。

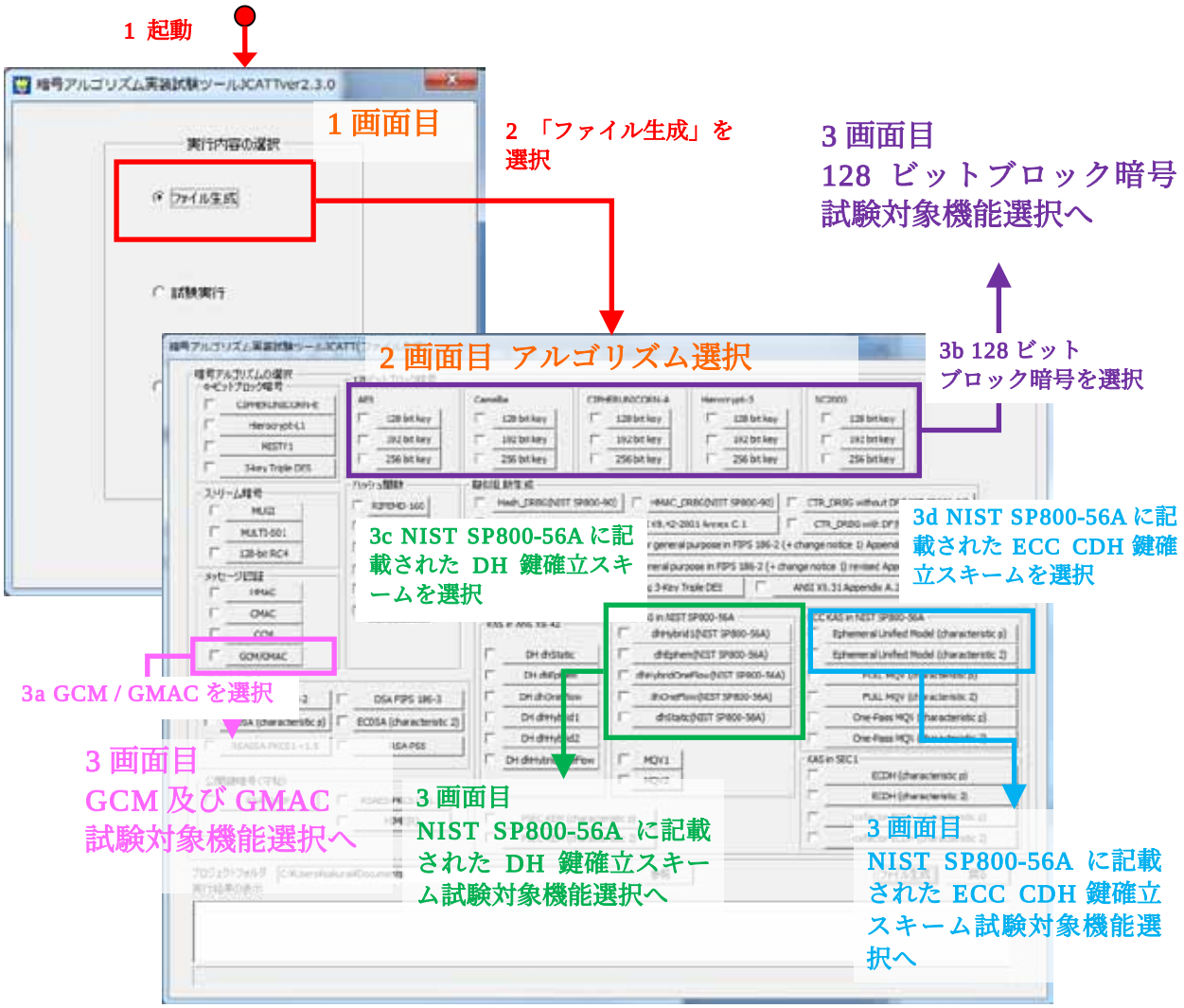
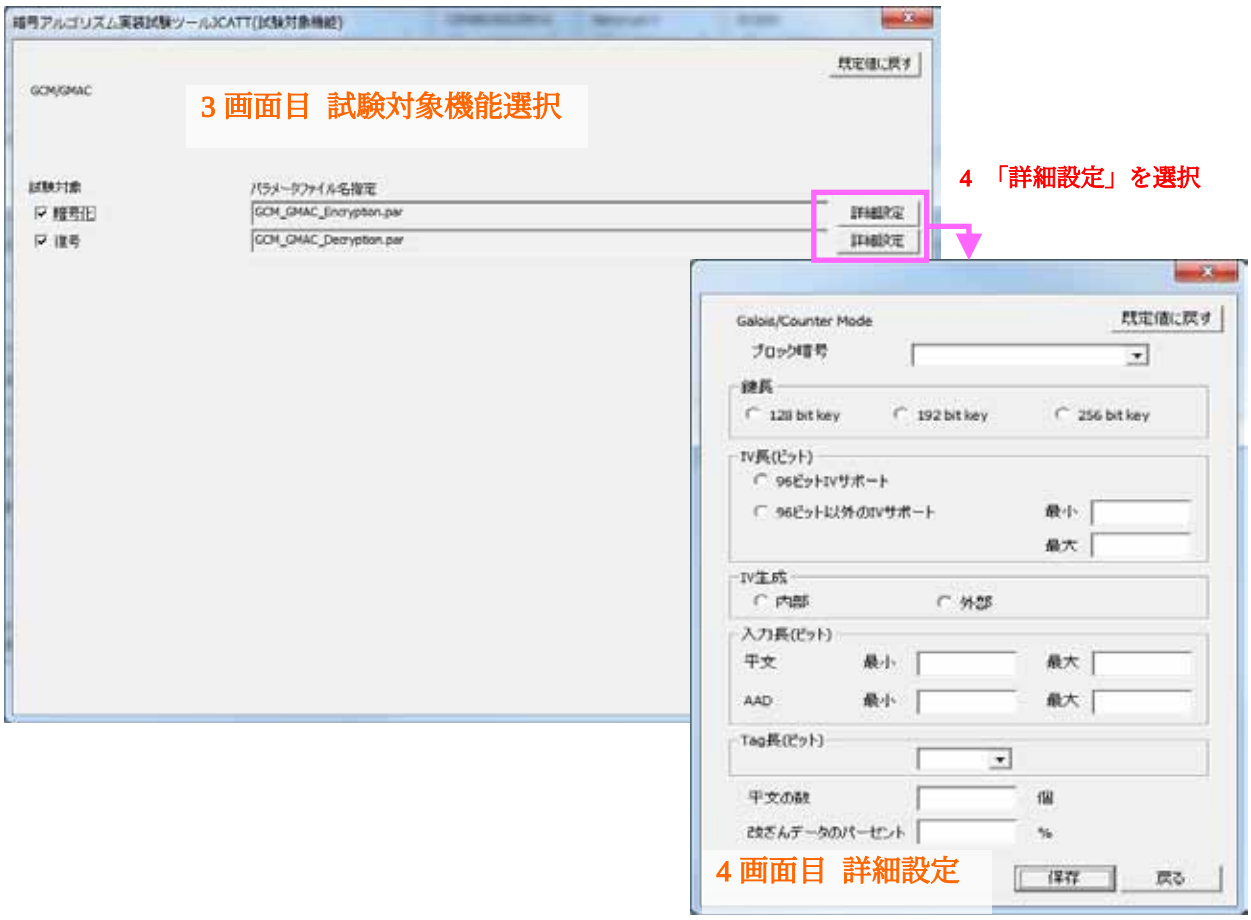


図 1 JCATT の画面構成 --起動から暗号アルゴリズム選択まで--

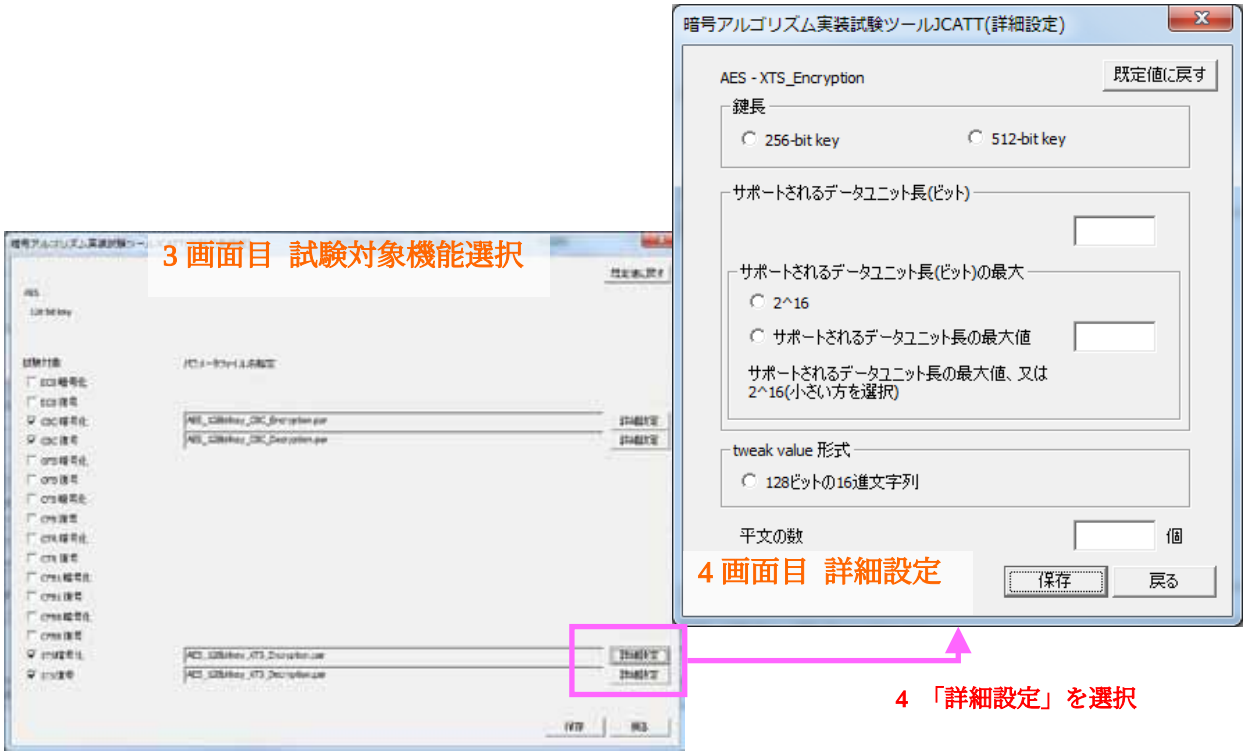
5.3.1.2. GCM 及び GMAC 試験対象機能選択

次に、試験対象機能として、今回開発対象である GCM 及び GMAC 選択時から、詳細設定画面までの画面遷移を以下に示す。

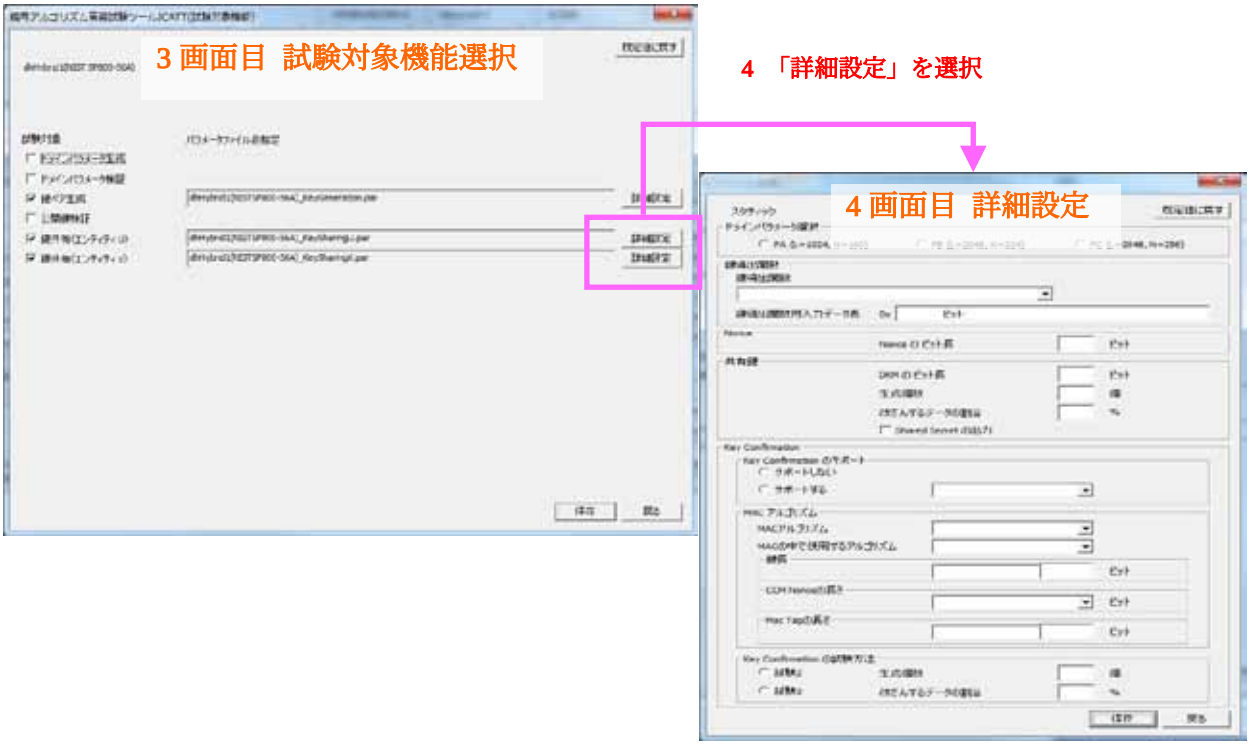


5.3.1.3. 128 ビットブロック暗号 試験対象機能選択

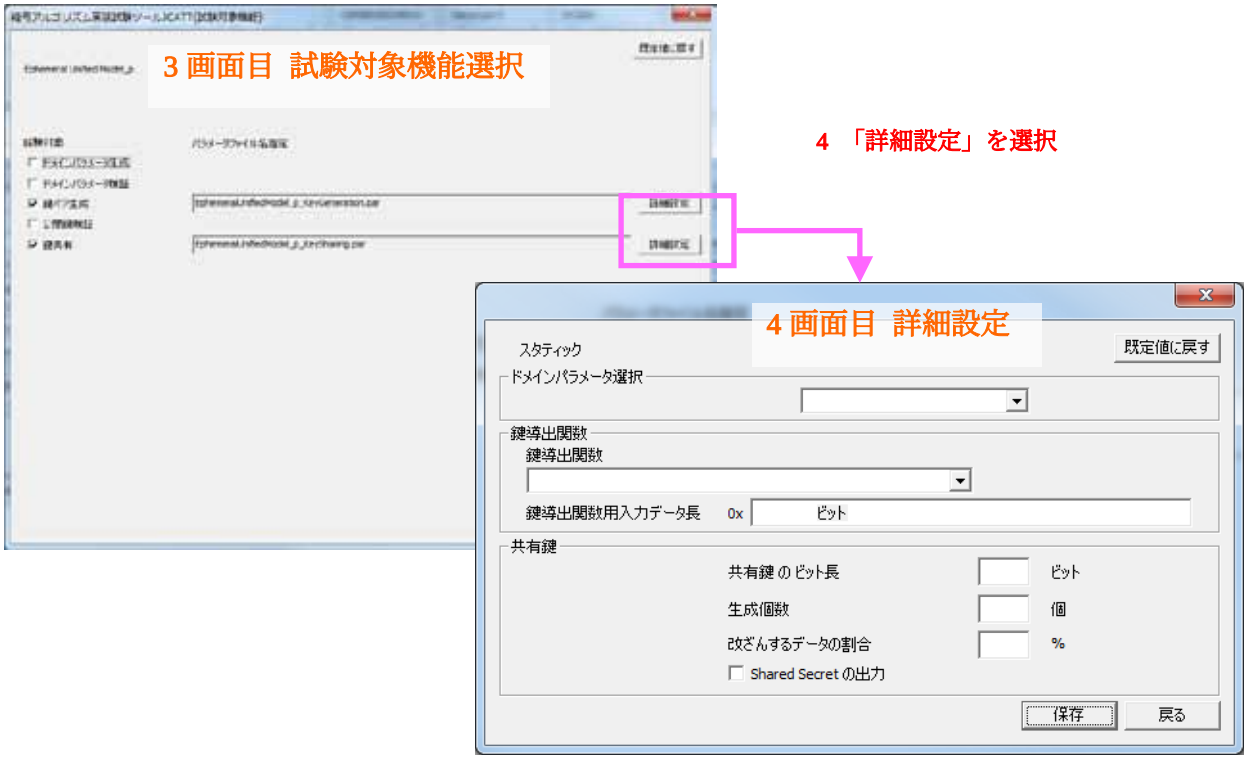
次に、試験対象機能として、128 ビットブロック暗号選択時から、XTS モード詳細設定画面までの画面遷移を以下に示す。



5.3.1.4. NIST SP800-56A に記載された DH 鍵確立スキーム 試験対象機能選択



5.3.1.5. NIST SP800-56A に記載された ECC CDH 鍵確立スキーム 試験対象機能選択



5.3.2. JCATT の GUI 改修内容詳細

本開発における試験機能の追加においては、JCATT のアルゴリズム選択画面に対して以下の改修を行う。

1. 「128 ビットブロック暗号」の各アルゴリズム(AES, Camellia, CIPHERUNICORN-A, Hierocrypt-3, SC2000)の、128 bit key および 256 bit key と書かれたボタンを押したとき

のパラメータ入力画面で、「XTS 暗号化」および「XTS 復号」を指定できるようにする。192 bit key ボタンから遷移する画面は変更しない。

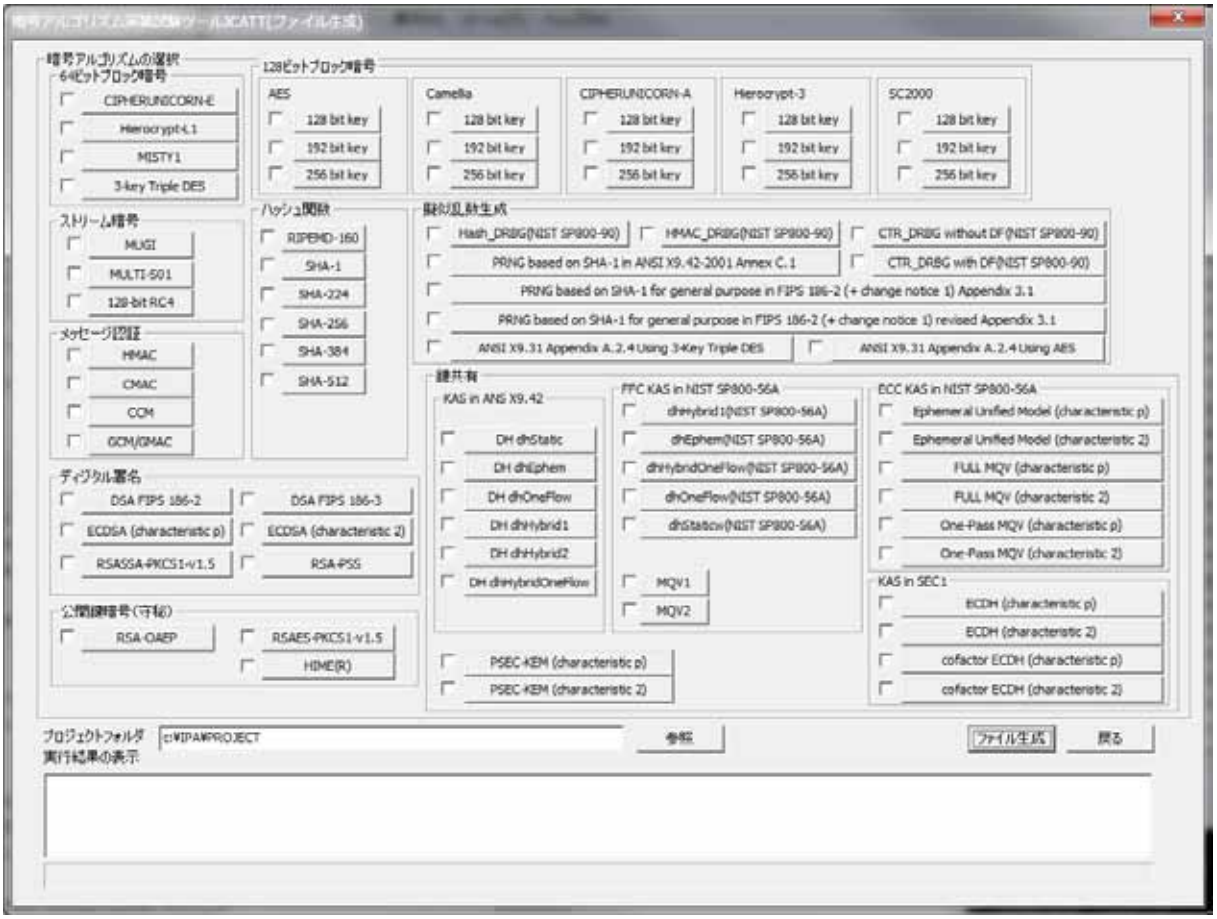
2. 「メッセージ認証」のグループに、”GCM/GMAC”と書かれたボタンを追加する。このボタンを押すと、GCM 試験の試験対象機能設定画面が表示される。
3. 「鍵共有」のグループの中に、「KAS in ANS X9.42」、「FFC KAS in NIST SP800-56A」、「ECC KAS in NIST SP800-56A」、「KAS in SEC1」というグループを作成する。
4. dhHybrid1、dhEphem、dhHybridOneFlow、dhOneFlow、dhStatic の 5 個のスキームに関して、”[スキーム名](NIST SP800-56A”と書かれたボタン(例: dhHybrid1(NIST SP800-56A))を追加する。さらに、”Ephemeral Unified Model (characteristic p)” 書かれたボタンおよび” Ephemeral Unified Model (characteristic 2)”と書かれたボタンを追加する。それぞれのボタンが属するグループは、表 3の通りとする。また、鍵共有グループの中に存在する既存のボタンの位置を移動し、属するグループを表 3の通りとする。” (characteristic p)”と” (characteristic 2)”の違いは、受け付けるドメインパラメータの定義体のタイプである。前者は GF(p)(p は素数)用、後者は GF(2^m)用である。

表 3 鍵共有グループ内のボタンの分類

グループ	ボタン	既存/新規
KAS in ANS X9.42	DH dhStatic	既存
	DH dhEphem	既存
	DH dhOneFlow	既存
	DH dhHybrid1	既存
	DH dhHybrid2	既存
	DH dhHybridOneFlow	既存
FFC KAS in NIST SP800-56A	dhHybrid1 (NIST SP800-56A)	新規
	dhEphem (NIST SP800-56A)	新規
	dhHybridOneFlow (NIST SP800-56A)	新規
	dhOneFlow (NIST SP800-56A)	新規
	dhStatic (NIST SP800-56A)	新規
ECC KAS in NIST SP800-56A	Ephemeral Unified Model (characteristic p)	新規
	Ephemeral Unified Model (characteristic 2)	新規
	FULL MQV (characteristic p)	既存
	FULL MQV (characteristic 2)	既存
	One-Pass MQV (characteristic p)	既存
	One-Pass MQV (characteristic 2)	既存
KAS in SEC1	ECDH (characteristic p)	既存
	ECDH (characteristic 2)	既存
	cofactor ECDH (characteristic p)	既存
	cofactor ECDH (characteristic 2)	既存
グループ外(鍵共有の直下)	PSEC-KEM (characteristic p)	既存
	PSEC-KEM (characteristic 2)	既存

追加あるいは改修する画面すべてについて、日本語及び英語のユーザインタフェースを提供する。言語の切り替えは、表 1にある通り、JCATT.ini ファイルで指定する。
新たに試験対象機能のボタンを追加した後のアルゴリズム選択画面は、図 2のようにする。

図 2: 機能追加後のアルゴリズム選択画面



試験対象選択画面は、現状の JCATT にある、他のアルゴリズム用の画面のテンプレート(図 3)を、プログラム中でラベル等の表示に対する必要な変更を施した上で表示する。ラベル等に表示する文字についての仕様は表 4の通りとする。また、128 ビットブロック暗号において、XTS 暗号化/復号の項目を表示する位置は、表 5の通りとする。試験対象機能選択画面においての、デフォルトでのチェックボックスの選択状態は、JCATT.ini ファイルで指定するが、インストール直後の JCATT.ini ファイルの内容は、選択状態が表 6の通りになるようにする。ラベルの英語表記については、表 7の通りとする。パラメータファイル名指定のテキストエリアおよび詳細設定ボタンは、チェックボックスがチェックされているときに表示し、チェックされていないときには非表示とする。

表 4 パラメータ設定画面の表示

	Galois/Counter Mode	FFC KAS in NIST SP800-56A (dhEphem 以外)	FFC KAS in NIST SP800-56A (dhEphem)	ECC KAS in NIST SP800-56A
ドメインパラメータファイル名指定	非表示	非表示	非表示	表示
ラベル(アルゴリズム)	Galois/Counter Mode	[スキーム名](SP800-56A)	dhEphem(SP8000-56A)	Ephemeral Unified Model_[体のタイプ(p あるいは 2)]
機能 1	GCM 暗号化	ドメインパラメータ生成	ドメインパラメータ生成	ドメインパラメータ生成
機能 2	GCM 復号	ドメインパラメータ検証	ドメインパラメータ検証	ドメインパラメータ検証
機能 3	非表示	鍵ペア生成	鍵ペア生成	鍵ペア生成
機能 4	非表示	公開鍵検証	公開鍵検証	公開鍵検証
機能 5	非表示	鍵共有(エンティティ U)	鍵共有	鍵共有
機能 6	非表示	鍵共有(エンティティ V)	非表示	非表示
機能 7 以降	非表示	非表示	非表示	非表示

表 5 128 ビットブロック暗号において XTS 暗号化/復号の項目を追加する位置

	AES	Camellia / CIPHERUNICORN-A / Hierocrypt-3 / SC2000
XTS 暗号化	機能 15	機能 11
XTS 復号	機能 16	機能 12

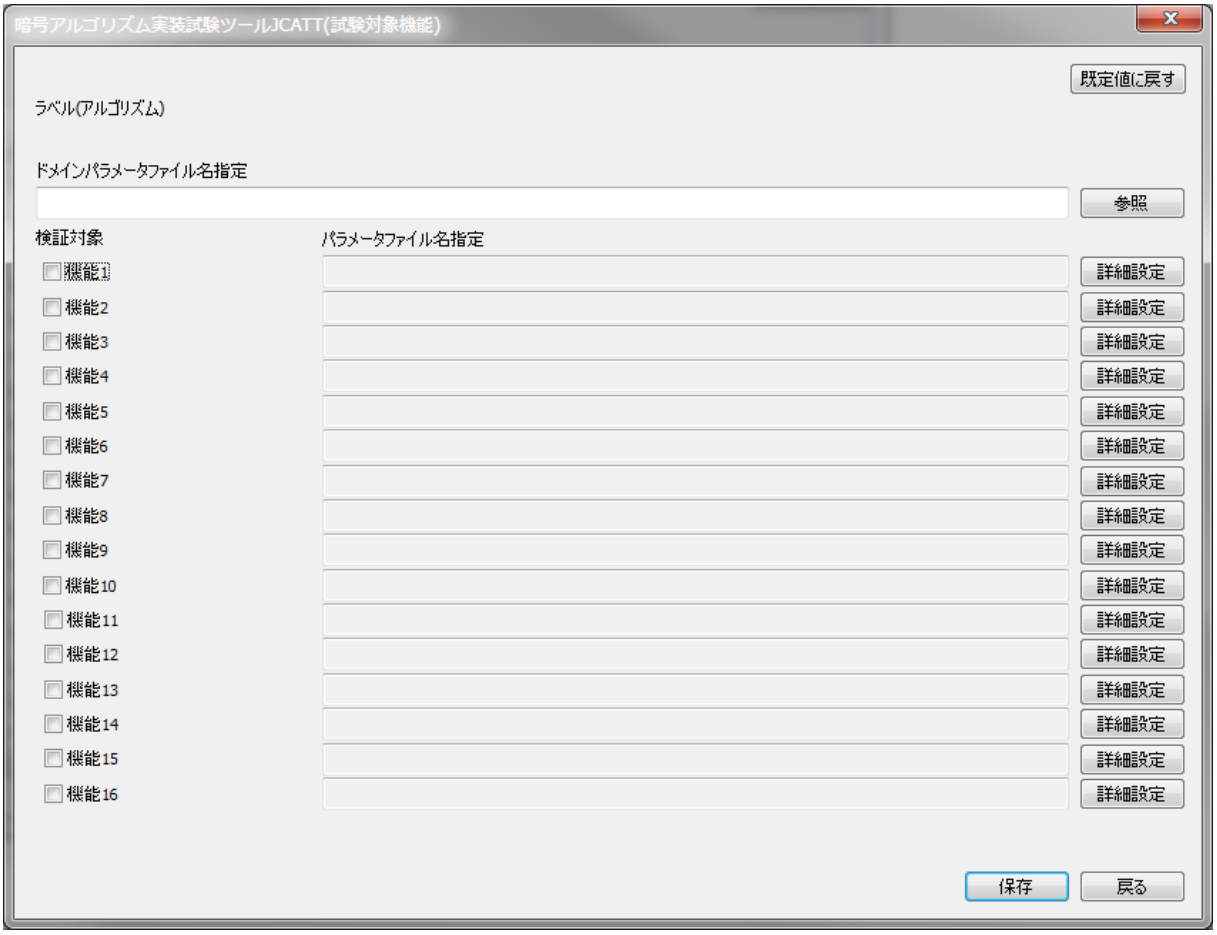
表 6 チェックボックスのチェック状態のデフォルト値(Y: チェックあり, N: チェックなし)

	Galois/Counter Mode	FFC KAS in NIST SP800-56A (dhEphem 以外)	FFC KAS in NIST SP800-56A (dhEphem)	ECC KAS in NIST SP800-56A
機能 1	Y	N	N	N
機能 2	Y	N	N	N
機能 3	-	Y	Y	Y
機能 4	-	Y	Y	Y
機能 5	-	Y	Y	Y
機能 6	-	Y	-	-

表 7 英語表記

日本語	英語
GCM 暗号化	GCM Encryption
GCM 復号	GCM Decryption
XTS 暗号化	XTS Encryption
XTS 復号	XTS Decryption
ドメインパラメータ生成	Domain parameters generation
ドメインパラメータ検証	Domain parameters validation
鍵ペア生成	Key generation
公開鍵検証	Public key validation
鍵共有	Key agreement
エンティティ	Entity

図 3 試験対象機能選択画面



5.3.3. GCM 及び GMAC の試験条件入力画面

GCM 及び GMAC の試験対象機能選択画面において、暗号化/復号をチェックして詳細設定ボタンを押した時に表示される試験条件入力画面を新規に作成する。試験条件入力画面は

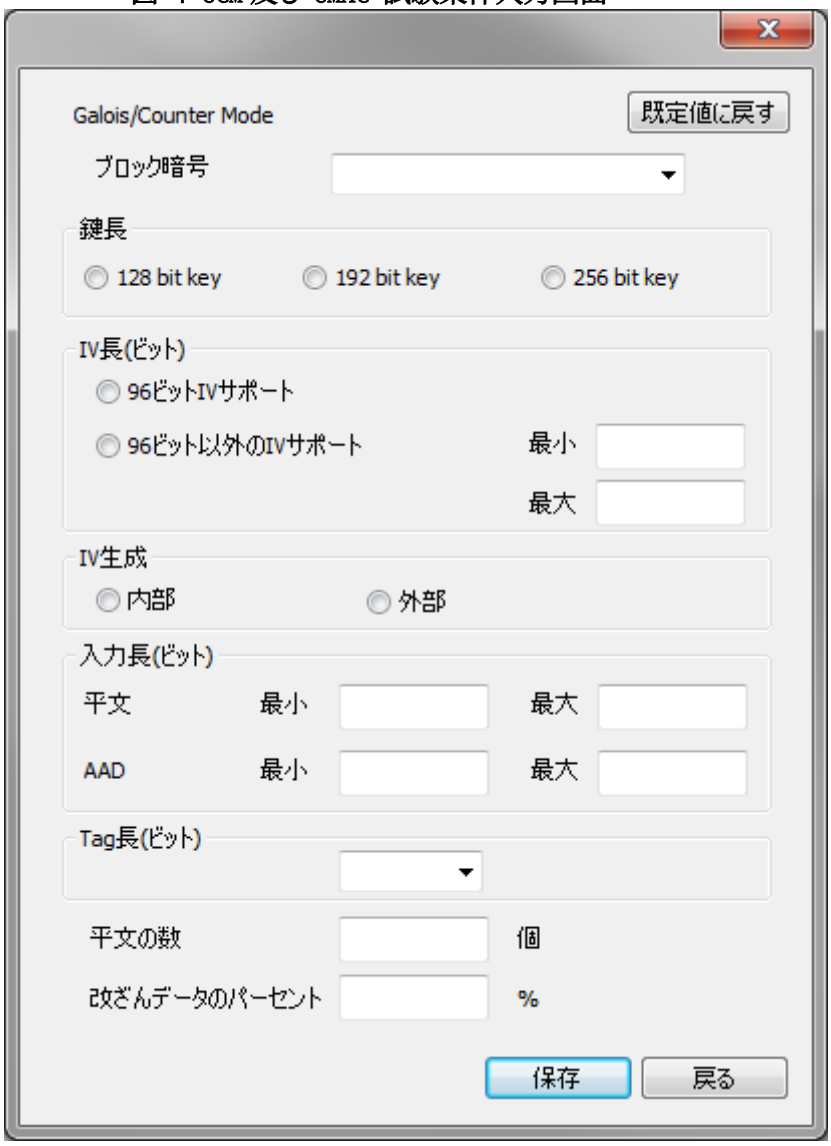
図 4の通りとし、画面上の各ウィジェットの機能は表 8の通りとする。

表 8 GCM 及び GMAC 試験条件入力画面の入力項目

種類	内容	機能
ラベル	試験対象機能	試験対象機能を表示する。暗号化の場合は”Galois/Counter Mode – Encryption”を、復号の場合は”Galois/Counter Mode – Decryption”を表示する。
ボタン	既定値に戻す	入力内容を既定値に戻す
ドロップダウンリスト	組み合わせる 128 ビットブロック暗号アルゴリズム	GCM と組み合わせる 128 ビットブロック暗号を選択できるドロップダウンリストとする。
ラジオボタン	鍵長	鍵長を、128 ビット、192 ビット、256 ビットの中から選択する。
ラジオボタン	96 ビット IV サポート	実装が 96 ビット長の IV をサポートし、その長さの IV に対して試験をする場合にチェックする
ラジオボタン	96 ビット長以外の IV サポート	実装が 96 ビット長以外の IV をサポートし、それに対して試験をする場合にチェックする
テキストエリア	最小	実装が 96 ビット長以外の IV をサポートし、それに対して試験をする場合に、サポートする IV 長(ビット)の最小値を指定する。
テキストエリア	最大	実装が 96 ビット長以外の IV をサポートし、それに対して試験をする場合に、サポートする IV 長(ビット)の最大値を指定する。
ラジオボタン	IV 生成	暗号化試験の場合にのみ表示させる。実装が暗号化の際に IV を外部生成とするか内部生成とするかを選択する。
テキストエリア	(平文の)入力長	暗号化の場合、平文の入力長の最小値と最大値を指定する。 復号の場合、暗号文の入力長の最小値と最大値を指定する。
テキストエリア	(AAD の)入力長	AAD(Additional Authenticated Data)の入力長の最小値と最大値を指定する。
ドロップダウンリスト	Tag 長	Tag 長を、GCM の仕様上許されている値から選択する。

		編集不可のドロップダウンリストとする。
テキストエリア	平文の数/暗号文の数	暗号化試験の場合は「平文の数」、復号試験の場合は「暗号文の数」とラベルに表示する。試験のために生成する暗号文あるいは平文の数を指定する。
テキストエリア	改ざんデータのパーセント	復号試験の場合にのみ表示させる。

図 4 GCM 及び GMAC 試験条件入力画面



5.3.4. XTS モードの試験条件入力画面

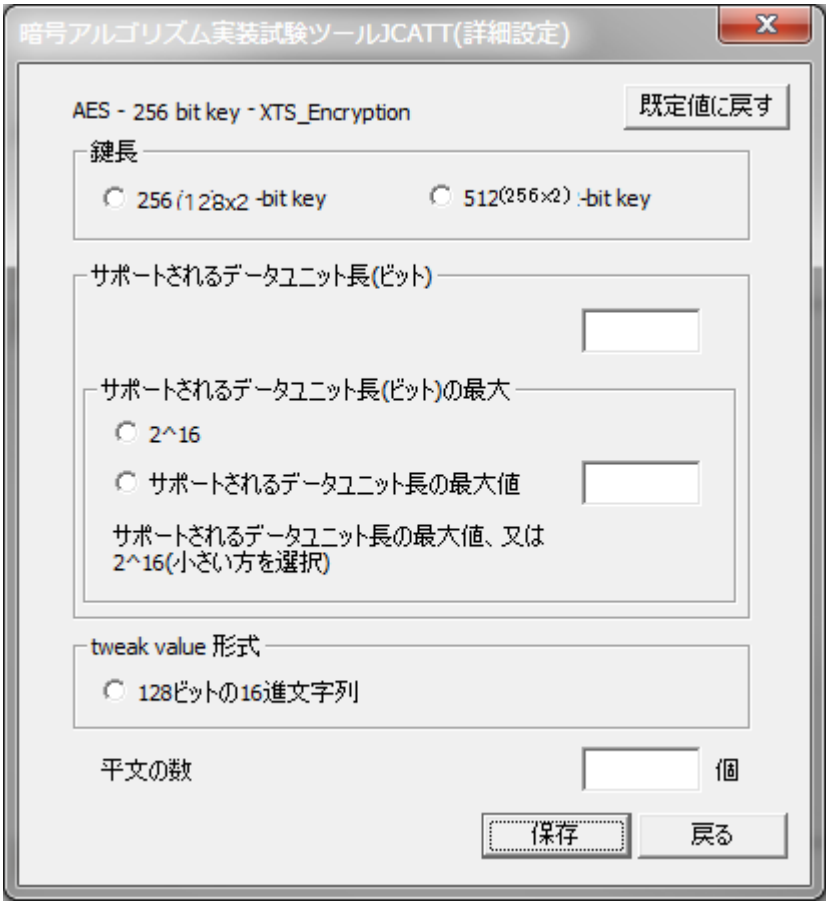
XTS モードの試験対象機能選択画面において、暗号化/復号をチェックして詳細設定ボタンを押した時に表示される試験条件入力画面を新規に作成する。試験条件入力画面は図 5の通りとし、画面上の各ウィジェットの機能は表 9の通りとする。

表 9 XTS モード 試験条件入力画面の入力項目

種類	内容	機能
ラベル	試験対象機能	試験対象機能を表示する。暗号化の場合は"[暗号プリミティブ名] – [鍵長] bit key - XTS_Encryption"を、復号の場合は" [暗号プリミティブ名] – [鍵長] bit key XTS_Decryption"を表示する(例: AES – 128 bit key - XTS_Encryption)。
ボタン	既定値に戻す	入力内容を既定値に戻す

ラジオボタン	鍵長	鍵長を、256(128x2)ビットと512(256x2)ビットから選択するラジオボタン。”128 bit key”ボタンを押して遷移した場合は”256(128x2)-bit key”が、”256 bit key”ボタンを押して遷移した場合は”512(256x2)-bit key”が選択された状態とし、ユーザによる選択変更は不可とする(表示専用)。
テキストエリア	サポートされるデータユニット長	実装によってサポートされ、アルゴリズム実装試験の対象とするデータユニット長(ビット)を指定する。
ラジオボタン	2^16 / サポートされるデータユニット長の最大値 の選択	実装によってサポートされるデータユニット長の最大値(ビット)と 2^16 のうち大きい方を選択する。実装によってサポートされるデータユニット長を選択した場合にのみその右に配置されたテキストエリアを活性化させる。
テキストエリア	サポートされるデータユニット長の最大値	前記のラジオボタンにおいて、サポートされるデータユニット長の最大値を選択した場合に入力可能とする。最大値の入力が選択されている場合、入力値が 2^16 以上の値でない場合はエラーとする。
テキストエリア	平文の数/暗号文の数	ラベルには、暗号機能の試験の場合には「平文の数」、復号機能の試験の場合には「暗号文の数」と表示する。試験において生成する平文あるいは暗号文の個数を指定する。

図 5 XTS モード 試験条件入力画面



「戻る」ボタンを押すと、入力データを内部に保存せずに試験対象機能選択画面に遷移する。「保存」ボタンを押すと、入力されたデータが条件を満たしていることをチェックする。条件を満たしていない場合には、満たしていない条件を表現するエラーメッセージを表示したダイアログを表示する。条件を満たしている場合、入力データを内部に保存して試験対象機能選択画面に遷移する。

5.3.5. FFC KAS in NIST SP800-56A 試験機能の試験条件入力画面

試験仕様に書かれたパラメータを入力できる GUI を JCATT に追加する。試験仕様に書かれた制約条件を満たさないパラメータが入力された場合は適切なエラーメッセージを表示したエラーダイアログを表示し、そのようなパラメータの入力を抑止すること。
各スキームの試験対象機能選択画面において、「ドメインパラメータ生成」「ドメインパラメータ検証」「鍵ペア生成」「公開鍵検証」の「詳細設定」ボタンを押したときの動作は、KAS in ANS X9.42 においてそれぞれ同名のボタンを押したときの動作と同様にする。
「鍵共有」(dhEphem 選択時のみ)、「鍵共有(エンティティ U)」「鍵共有(エンティティ V)」(dhEphem 以外のスキームを選択時)の「詳細設定」ボタンが押された時には、図 6の通りの試験条件入力画面を表示する。画面上の各ウィジェットの機能は、表 10の通りとする。

表 10 FFC KAS in NIST SP800-56A 試験条件入力画面の入力項目

種類	内容	動作/機能
ラベル	試験対象機能	試験対象機能を表示する。”DH [スキーム名] - Key agreement” と表示する(例: dhHybrid1 – Key agreement)
ボタン	既定値に戻す	入力内容を既定値に戻す
ボタン	保存	画面の入力内容を.ini ファイル

		に保存する。
ボタン	戻る	画面の入力内容をファイル保存せずに、ダイアログを閉じる。
ラジオボタン	ドメインパラメータ選択	ドメインパラメータのビット長。FA,FB,FC から選択する。
ドロップダウンボックス	鍵導出関数	鍵導出関数(KDF)を、NIST SP800-56A の 5.8.1 及び 5.8.2 に挙げられているものとハッシュ関数を組み合わせた選択肢を提示して選択させる。それに加えて、”None”も選択肢に入れる。 “None”は、鍵導出関数(KDF)を使用せず、Shared Secret を用いて試験を行うことを意味する。 ただし、ドメインパラメータの選択によって組み合わせるハッシュが限定されるので、実際には指定されたドメインパラメータにおいて選択不可のものは選択肢から除外すること。
テキストエリア	鍵導出関数用入力データ長	鍵導出関数に入力する”Other Info”のデータのビット長を入力する。
テキストエリア	IUTid	OtherInfo を生成するための、IUT の ID を 16 進文字列で入力する。
テキストエリア	Nonce のビット長	Nonce のビット長を入力する。Nonce が必要なスキーム(dhStatic)の場合にのみ活性化し、それ以外のスキームの場合には非活性とする。
テキストエリア	DKM のビット長	生成する DKM のビット長を指定する。KDF が None の場合には非活性とする。
テキストエリア	(共有鍵)生成個数	試験データの生成個数を指定する。
テキストエリア	(共有鍵)改ざんするデータの割合	生成する試験データのうち、検証結果が不合格となるデータの割合をパーセントで指定する
ラジオボタン	DKM による検証	試験 1 の検証方法を選択するためのラジオボタン。 こちらを選択された場合で、Key Confirmation をサポートしない場合、次の項目を非活性化させること。
ラジオボタン	MacTag による検証	試験 1 の検証方法を選択するためのラジオボタン。 こちらが選択された場合、次の項目を活性化させること。 l　MAC アルゴリズム

		l MAC で使用するアルゴリズム l 鍵長 l CCM Nonce の長さ l MacTag の長さ
ドロップダウンリスト	MAC アルゴリズム	Key Confirmation 及び試験 1 の MacTag による検証で使用する MAC アルゴリズムを、 CMAC CCM HMAC から選択させる
ドロップダウンリスト	MAC で使用するアルゴリズム	MAC アルゴリズムが CCM の場合、使用するブロック暗号アルゴリズムを以下から選択させる。 AES Camellia CIPHERUNICORN-A Hierocrypt-3 SC2000 MAC アルゴリズムが CMAC の場合、選択肢が AES1 個のみのドロップダウンリストを表示する。 MAC アルゴリズムが HMAC の場合、使用するハッシュアルゴリズムを以下から選択させる。 SHA1 SHA224 SHA256 SHA384 SHA512 ただし、ドメインパラメータの選択によって使用可能なハッシュが限定されるので、実際には指定されたドメインパラメータにおいて選択不可のものは選択肢から除外すること。
テキストエリア あるいはドロップダウンリスト	鍵長	MAC 鍵の長さを指定させる。 MAC アルゴリズムが CMAC 又は CCM の場合、128,192,256 から選択させるドロップダウンリストを表示する。HMAC の場合、テキストエリアを表示する。 ただし、ドメインパラメータの選択によって使用可能な鍵長が限定されるので、実際には指定されたドメインパラメータにおいて、ドロップダウンリストから選択不可のものは選択肢から除外し、テキストエリアについては入力チェックを行うこと。
テキストエリア	CCM Nonce の長さ	MAC アルゴリズムが CCM の場

		合のみ活性化させる。CCM Nonce の長さをドロップダウンリストで選択させる。
テキストエリア あるいはドロップダウンリスト	Mac Tag の長さ	出力する Mac Tag の長さを指定させる。MAC アルゴリズムが CCM あるいは CMAC の場合選択したドメインパラメータ(FA,FB,FC)に応じて選択可能な候補からドロップダウンリストで選択させる。HMAC の場合、テキストエリアを表示する。ただし、ドメインパラメータの選択によって使用可能な Mac Tag の長さが限定されるので、テキストエリアについては入力チェックを行うこと。
ラジオボタン	Key Confirmation のサポート	Key Confirmation をサポートするかどうかを、「サポートする」「サポートしない」から選択させる。「サポートしない」を選択した場合、Key Confirmation グループにある、Key Confirmation サポートの選択以外のすべてのウィジェットを非活性化する。 dhEphem 選択時には、Key Confirmation を「サポートしない」のみ選択可能。 (「サポートする」は仕様上あり得ない。)
ドロップダウンリスト	Key Confirmation の種類	Key Confirmation の種類を選択させる。 Unilateral U to V Unilateral V to U Bilateral から選択可能とする。
ラジオボタン	試験 2/試験 3	Key Confirmation の種類が Unilateral の場合は試験 2 を、Bilateral の場合は試験 3 を自動的に選択させる。ユーザによるこのラジオボタンの直接操作は不可とする。
テキストエリア	(Key Confirmation の試験)生成個数	Key Confirmation の試験における試験データの生成個数を入力する。
テキストエリア	(Key Confirmation の試験)改ざんするデータの割合	Key Confirmation の試験における試験データにおいて、誤った Tag を出力する割合をパーセントで入力する。

図 6 FFC KAS in NIST SP800-56A 試験条件入力画面

「保存」ボタンは、上記で入力したパラメータを保存する機能を持つボタンである。ただし、「JCATT ファイルフォーマット仕様書」「暗号アルゴリズム実装試験仕様書」に記載された条件を満たさないパラメータが入力されている場合には、どのパラメータが条件を満たしていないかを示すエラーメッセージを表示されたダイアログを表示し、画面遷移を抑止する。

5.3.6. ECC KAS in NIST SP800-56A 試験機能の試験対象機能選択画面

ECC KAS in NIST SP800-56A の試験対象機能選択画面は、表 4、表 6、及び表 7の仕様に従うものとする。
ただし、「詳細設定画面」を押した際に、指定されたドメインパラメータの定義体のタイプが正しいことをチェックすること。”Ephemeral Unified Model (characteristic p)”ボタンが押されて遷移した場合は、定義体が GF(p)(pは素数)であるかどうかを、”Ephemeral Unified Model (characteristic 2)”ボタンが押されて遷移した場合は、定義体が GF(2^m)であるかどうかをチェックすること。タイプが正しくない場合はエラーメッセージを表示させる。定義体のタイプが正しい場合、さらにドメインパラメータが EA, EB, EC, ED, EE(NIST SP800-56A の 5.5.1.2 Table 2 を参照)のいずれに属するかを判定し、次画面への遷移時に反映させる。分類不能の場合はエラーメッセージを表示させる。

5.3.7. ECC KAS in NIST SP800-56A 試験機能の試験条件入力画面

ECC KAS in NIST SP800-56A の試験対象選択画面において、「鍵共有」の「詳細設定」ボタンが押された時には、図 7の通りの試験条件入力画面を表示する。画面上の各ウィジェットの機能は、表 11の通りとする。

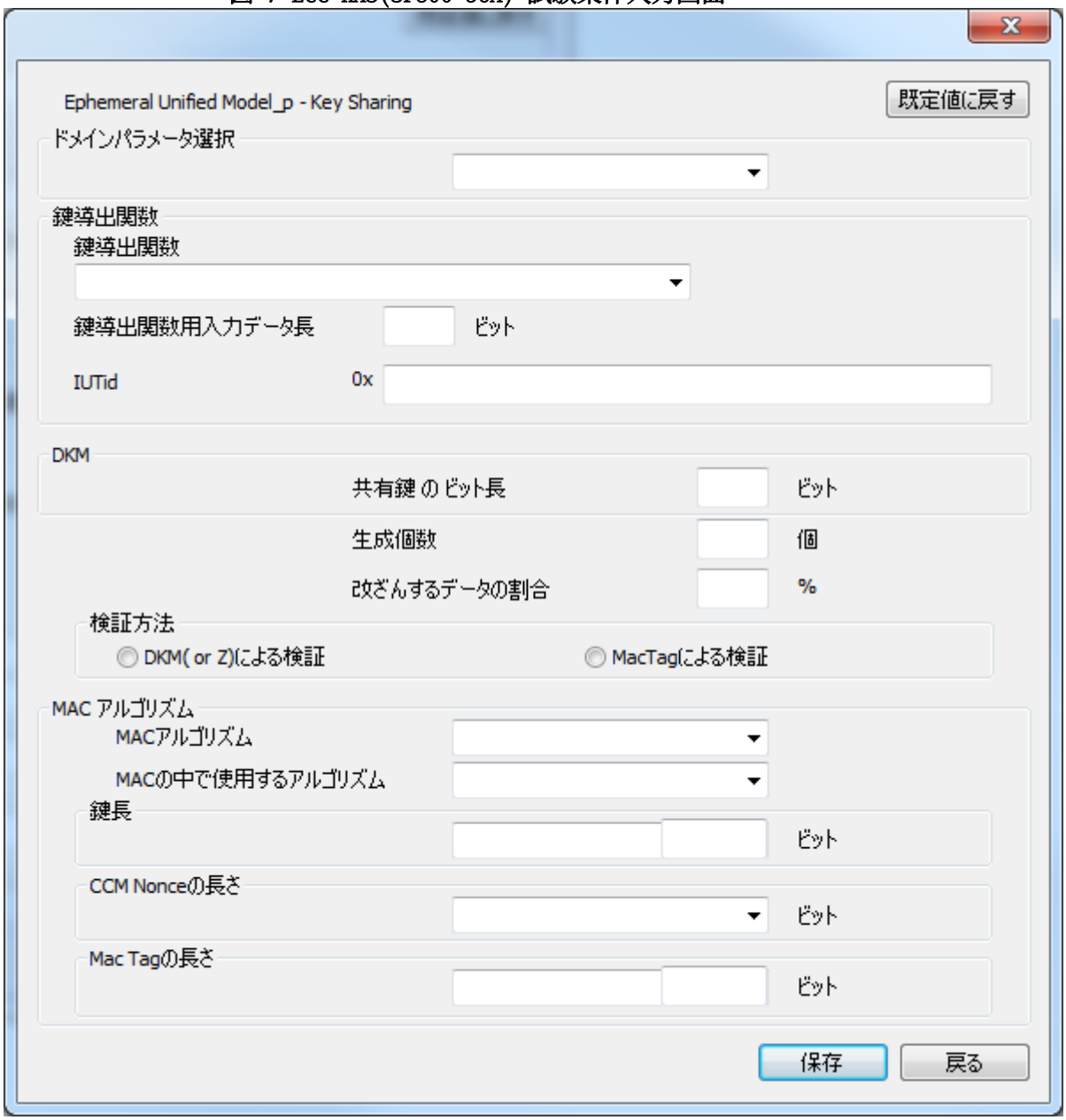
表 11 ECC KAS(NIST SP800-56A) 試験条件入力画面の入力項目

種類	内容	機能
ラベル	試験対象機能	
ボタン	保存	画面の入力内容を.ini ファイルに保存する。
ボタン	戻る	画面の入力内容をファイル保存せずに、ダイアログを閉じる。
ボタン	既定値に戻す	入力内容を既定値に戻す
ラジオボタン	ドメインパラメータ選択	パラメータ入力画面で選択したドメインパラメータのファイルの内容から、そのパラメータセットが EA, EB, EC, ED, EE のどれに属するかを判断して表示させる。
ドロップダウンボックス	鍵導出関数	鍵導出関数(KDF)を、NIST SP800-56A の 5.8.1 及び 5.8.2 に挙げられているものとハッシュ関数を組み合わせた選択肢を提示して選択させる。それに加えて、”None”も選択肢に入れる。 “None”は、鍵導出関数(KDF)を使用せず、Shared Secret を用いて試験を行うことを意味する。 ただし、ドメインパラメータの選択によって組み合わせるハッシュが限定されるので、実際には指定されたドメインパラメータにおいて選択不可のものは選択肢から除外すること。
テキストエリア	鍵導出関数用入力データ長	鍵導出関数に入力する”Other Info”のデータのビット長を入

		力する。
テキストエリア	IUTid	OtherInfo を生成するための、IUT の ID を 16 進文字列で入力する。
テキストエリア	DKM のビット長	生成する DKM のビット長を指定する。KDF が None の場合には非活性とする。
テキストエリア	(共有鍵)生成個数	試験データの生成個数を指定する
テキストエリア	(共有鍵)改ざんするデータの割合	生成する試験データのうち、検証結果が不合格となるデータの割合をパーセントで指定する
ラジオボタン	DKM による検証	検証方法を選択するためのラジオボタン。 こちらを選択された場合、次の項目を非活性化させること。
ラジオボタン	MacTag による検証	検証方法を選択するためのラジオボタン。 こちらを選択された場合、次の項目を活性化させること。 l MAC アルゴリズム l MAC で使用するアルゴリズム l 鍵長 l CCM Nonce の長さ l MacTag の長さ
ドロップダウンリスト	MAC アルゴリズム	MacTag による検証で使用する MAC アルゴリズムを、 l CMAC l CCM l HMAC から選択させる
ドロップダウンリスト	MAC で使用するアルゴリズム	MAC アルゴリズムが CCM の場合、使用するブロック暗号アルゴリズムを以下から選択させる。 l AES l Camellia l CIPHERUNICORN-A l Hierocrypt-3 l SC2000 MAC アルゴリズムが CMAC の場合、選択肢が AES1 個のみのドロップダウンリストを表示する。 MAC アルゴリズムが HMAC の場合、使用するハッシュアルゴリズムを以下から選択させる。 l SHA1 l SHA224 l SHA256

		｜ SHA384 ｜ SHA512 ただし、ドメインパラメータの選択によって使用可能なハッシュが限定されるので、実際には指定されたドメインパラメータにおいて選択不可のものは選択肢から除外すること。
テキストエリア あるいはドロップダウンリスト	鍵長	MAC 鍵の長さを指定させる。MAC アルゴリズムが CMAC 又は CCM の場合、128,192,256 から選択させるドロップダウンリストを表示する。HMAC の場合、テキストエリアを表示する。 ただし、ドメインパラメータの選択によって使用可能な鍵長が限定されるので、実際には指定されたドメインパラメータにおいて、ドロップダウンリストから選択不可のものは選択肢から除外し、テキストエリアについては入力チェックを行うこと。
テキストエリア	CCM Nonce の長さ	MAC アルゴリズムが CCM の場合のみ活性化させる。CCM Nonce の長さをドロップダウンリストで選択させる。
テキストエリア あるいはドロップダウンリスト	Mac Tag の長さ	出力する Mac Tag の長さを指定させる。MAC アルゴリズムが CCM あるいは CMAC の場合選択したドメインパラメータ(FA,FB,FC)に応じて選択可能な候補からドロップダウンリストで選択させる。HMAC の場合、テキストエリアを表示する。 ただし、ドメインパラメータの選択によって使用可能な Mac Tag の長さが限定されるので、テキストエリアについては入力チェックを行うこと。

図 7 ECC KAS(SP800-56A) 試験条件入力画面



「保存」ボタンは、上記で入力したパラメータを保存する機能を持つボタンである。ただし、「JCATT ファイルフォーマット仕様書」「暗号アルゴリズム実装試験仕様書」に記載された条件を満たさないパラメータが入力されている場合には、どのパラメータが条件を満たしていないかを示すエラーメッセージを表示されたダイアログを表示し、画面遷移を抑止する。

5.4. 試験ツールの完全性、不正改造検出機能

暗号アルゴリズムを用いた完全性確認技術であるメッセージ認証子を使用して、本試験ツールの完全性の確認及びその不正改造を検出する機能を実装すること。

5.4.1. メッセージ認証子ファイル生成機能

完全性の確認及びその不正改造を検出するために使用するメッセージ認証子をファイル出力できること。本機能を実装するために、以下の処理を実装すること。

(1) 画面から以下の情報を入力する。

ｌ　JCATT をインストールする PC の MAC アドレス(Media Access Control Address)

l　認証機関が任意に設定するパスワード
(2) (1)で入力したパスワードを以下の鍵導出関数 (KDF：Key Derivation Function) に入力して 128-bit の鍵を生成する。
l　ANSI X9.42 KDF with SHA-1 based on Concatenation
(3) (2)で生成した 128-bit の鍵と以下の情報を入力メッセージとして AES-CBC-MAC アルゴリズムによるメッセージ認証子を計算する。

読み込み順序	情報	属性
1	JCATT.exe	バイナリファイル
2	CryptoAlgorithms.dll	バイナリファイル
3	HC3.dll	バイナリファイル
4	HCL1.dll	バイナリファイル
5	unie.dll	バイナリファイル
6	unia128.dll	バイナリファイル
7	unia192.dll	バイナリファイル
8	unia256.dll	バイナリファイル
9	DLL_CIPHERUNICORNA128.dll	バイナリファイル
10	DLL_CIPHERUNICORNA192.dll	バイナリファイル
11	DLL_CIPHERUNICORNA256.dll	バイナリファイル
12	DLL_CIPHERUNICORNE.dll	バイナリファイル
13	DLL_Hierocrypto.dll	バイナリファイル
14	DLL_HIME.dll	バイナリファイル
15	DLL_MUGI.dll	バイナリファイル
16	DLL_MULTIS01.dll	バイナリファイル
17	DLL_PSEC.dll	バイナリファイル
18	DLL_SC2000.dll	バイナリファイル
19	ValidSys.exe	バイナリファイル
20	DLL_DRBG.dll	バイナリファイル
21	ASF01.dll	バイナリファイル
22	PC の MAC アドレス	メモリ上のデータ

(4) (3)で計算したメッセージ認証子を JCATT_MAC.txt ファイルに出力する。このとき、メッセージ認証子の出力形式は、16 進出力とすること。

ただし、(1)～(4)の基本機能は現行の JCATT に実装されている。本開発での開発範囲は、(3)における入力ファイルの追加のみである。

5.4.2. メッセージ認証子ファイル検証機能

メッセージ認証子をファイルから読み込み、本ツールを構成する実行形式から計算されるメッセージ認証子ファイルと異なる場合には、本ツールは起動出来なくなること。本機能を実装するために、以下の処理を実装すること。
(1) JCATT.exe 内部に5.4.1 (2)で生成した 128-bit の鍵を格納しておく。
(2) (1)の 128-bit の鍵と5.4.1 (3)に記載した情報を入力メッセージとしてAES-CBC-MAC アルゴリズムによるメッセージ認証子を計算する。
(3) JCATT_MAC.txt ファイルから読み込んだメッセージ認証子と(2)のメッセージ認証子を比較し、異なる場合には JCATT.exe は強制終了する。

ただし、(1)～(3)の基本機能は現行の JCATT に実装されている。本開発での開発範囲は、(2)における入力ファイルの追加のみである。

5.5. 性能要件

性能要件は、「ファイル生成」ボタンあるいは「試験実行」ボタンを押下したときの応答時間

が、Core2Duo プロセッサ(クロック 2.0GHz)、メモリ 1024MB の環境下で、以下で示す条件を満たすことである。

GCM 及び GMAC の試験機能に関する応答時間の要件は、表 12の通り。

表 12 GCM 及び GMAC の試験機能に関する応答時間

画面上の操作	応答時間	備考
ファイル生成	10 秒以内	生成個数が 10 個の場合。
試験実行(復号試験で、かつ IV が内部生成である場合を除く)	5 秒以内	
試験実行(復号試験で、かつ IV が内部生成である場合)	15 秒以内	

XTS モードの試験機能に関する応答時間の要件は、表 13の通り。

表 13 XTS モードの試験機能に関する応答時間

画面上の操作	応答時間	備考
ファイル生成	20 秒以内	データユニット長と最大データユニット長を 4096 ビットに設定し、平文(又は暗号文)の数を 10 個に設定した場合
試験実行	10 秒以内	

鍵確立手法の試験機能に関する応答時間の要件は、FFC KAS に関しては表 14の通り。ECC KAS に関しては表 15の通り。

表 14 鍵確立手法の試験機能に関する応答時間(FFC)

試験対象機能	画面上の操作	応答時間	備考
ドメインパラメータ生成	ファイル生成	5 秒以内	FA 選択時で、生成個数が 10 個の場合。
	試験実行	50 秒以内	
ドメインパラメータ検証	ファイル生成	50 秒以内	FA 選択時で、検証個数が 10 個の場合。
	試験実行	5 秒以内	
鍵ペア生成	ファイル生成	5 秒以内	FA 選択時で、生成個数が 10 個の場合。
	試験実行	5 秒以内	
公開鍵検証	ファイル生成	5 秒以内	FA 選択時で、検証個数が 10 個の場合。
	試験実行	5 秒以内	
鍵共有	ファイル生成	30 秒以内	FA 選択時で、dhHybrid1 選択時で、生成個数が 10 個の場合。
	試験実行	15 秒以内	

表 15 鍵確立手法の試験機能に関する応答時間(ECC)

試験対象機能	画面上の操作	応答時間	備考
ドメインパラメータ生成	ファイル生成	2 秒以内	EA 選択時で、生成個数が 10 個の場合。
	試験実行	50 秒以内	
ドメインパラメータ検証	ファイル生成	50 秒以内	EA 選択時で、検証個数が 10 個の場合。
	試験実行	5 秒以内	
鍵ペア生成	ファイル生成	5 秒以内	EA 選択時で、生成個数が 10 個の場合。
	試験実行	5 秒以内	
公開鍵検証	ファイル生成	5 秒以内	EA 選択時で、検証個数が 10 個の場合。
	試験実行	5 秒以内	
鍵共有	ファイル生成	30 秒以内	EA 選択時で、生成個数が 10 個の場合。
	試験実行	15 秒以内	

6. ドキュメント

6.1. 取扱説明書

6.1.1. 日本語の取扱説明書

現状の取扱説明書に今回機能追加した部分を含めた形で納品すること。ファイルフォーマットは、Microsoft Office Word 形式とすること。

6.1.2. 英語の取扱説明書

6.1.1の日本語の取扱説明書を英訳したものとすること。ファイルフォーマットは、Microsoft Office Word 形式とすること。

6.2. JCATT ファイルフォーマット仕様書

今回開発する試験機能で入出力する JCATT ファイルフォーマット仕様書を作成すること。

- JCATT ファイルフォーマット仕様書は、PDF フォーマットとすること。
- JCATT ファイルフォーマット仕様書のソースファイルは、LaTeX で記述すること。
- 分割単位は、次のとおりとすること。
  - GCM 及び GMAC
  - XTS モード
  - NIST SP800-56A に記載された FFC DH 鍵確立スキーム
  - NIST SP800-56A に記載された ECC CDH 鍵確立スキーム

JCATT ファイルフォーマット仕様書の形式は、現在下記の URL で公開している JCATT ファイルフォーマットと同様にすること。なお、現在公開している JCATT ファイルフォーマット仕様書の LaTeX ソースファイルについては本開発を行う者に開示する。
http://www.ipa.go.jp/security/jcmvp/open_documents.html

6.3. 暗号アルゴリズム実装試験仕様書

今回開発する試験機能で実装される暗号アルゴリズム実装試験仕様書を作成すること。
現在下記の URL で公開している暗号アルゴリズム実装試験仕様書に対して記述を追加する方式で行うこと。これらの仕様書の既存の版の LaTeX ソースファイルは本開発を行う者に開示する。
http://www.ipa.go.jp/security/jcmvp/open_documents.html
追加先のドキュメントは、下記の表のとおりとする。

GCM 及び GMAC	ATR-01-D
XTS モード	ATR-01-B
SP800-56A に基づく鍵確立手法	ATR-01-F

個々のドキュメントに対する具体的な仕様の記述の追加方法については、本開発を行うものに IPA が雛型を提供するので、それに従うこと。

6.4. JCATT が入出力するファイルのサンプル

3.1.1に記載した入出力ファイルのサンプルを作成すること。サンプルを作成する手順は以下のとおりである。

(1) パラメータファイル、質問ファイル、正解ファイルを JCATT に出力させる。
(2) (1)で作成したファイルに対して、暗号アルゴリズム実装試験が合格になるような回答ファイルを作成する。

(3) (1)(2)で作成したファイルを指定して、「試験実行」を行い、JCATT に結果ファイルを出力させる。

以上の手順によって、今回開発するすべての試験機能に対してサンプルを作成すること。

7. テスト

開発作業中または作業後にテストを行い、発見された問題について対応し解消すること。テストにあたっては、検証方法、指標、目標値に関して効果的かつ効率的な方針を立案すること。発見された問題及びそれに対応する作業の管理方針についても、プロジェクト計画に含めて立案すること。

- テスト計画を立案し、納入前に適切なテストを実施すること。
- IPA は、少なくとも以下のテストが実施されることを想定している。これによらない場合には、その旨提案すること。
  - 詳細設計に基づく単体テスト
  - 基本設計に基づく結合テスト
  - 発注仕様に基づくシステムテスト
  - 同値分割、境界値分析の手法を用いた正常系および異常系のテスト。
- 画面のテストにおいては、すべての入力パラメータに対する入力値チェックが機能することのテストを行うこと。
- 暗号アルゴリズムの実装のテストにおいては、少なくとも、第三者機関が公開している既知解データ(テストベクトル)を用いたテストを行うこと。例としては、NISTが公開しているテストベクトル[4]がある。

8. 事業の実施体制

(1) 実施要員に、暗号アルゴリズムに精通している者を含めること。

(2) PMBOK、EVM に基づいたプロジェクト管理等により、作業計画を明確に定め、作業項目毎の工程管理を行い、進捗状況を定期的に IPA 担当者に報告すること。また、作業の遅延等が生じた際には速やかに IPA 担当者に報告すること。

9. 事業期間及びスケジュール

(1) 事業期間

契約締結日から最終納入日まで

(2) スケジュール

作業計画の詳細については、契約締結後に別途 IPA と相談の上、IPA が承認するものとする。

10. 検収関連事項

10.1. 納入期限

納入は、機能別に 2 回に分割して行う。

[4] http://csrc.nist.gov/groups/STM/cavp/index.html

(1) 中間納入期限

納期は契約締結日の 3 か月後(ただし、その日が休日の場合は翌営業日)とする。

(2) 最終納入期限

納期は契約締結日の 9 か月後(ただし、その日が休日の場合は翌営業日)とする。

10.2. 納入場所

東京都文京区本駒込二丁目 28 番 8 号

独立行政法人 情報処理推進機構 セキュリティセンター

10.3. 納入物件

(1) 中間納入物件

本仕様書で定義された機能のうち、「GCM 及び GMAC」及び「XTS モード」の機能に関する部分を対象とする。

- 以下記載の文書等を収めた記録媒体(CD-R 又は DVD-R)一式
  - ① 暗号アルゴリズム実装試験ツール(JCATT)取扱説明書(日本語版及び英語版)
  - ② 暗号アルゴリズム実装試験仕様書
  - ③ JCATT ファイルフォーマット仕様書
  - ④ ②③の生成に必要な LaTeX ソースファイル
  - ⑤ テスト報告書、障害管理表(障害内容と対処内容の一覧表)
  - ⑥ 設計資料(基本設計書、詳細設計書)
  - ⑦ 納入物件一覧リスト及びソースコード一覧リスト
  - ⑧ JCATT が入出力するファイルのサンプル
  - ⑨ JCATT のソースコード及び実行形式生成に必要なファイル
  - ⑩ JCATT の実行用ロードモジュール
- 上記資料①～③、⑤～⑥の紙媒体各 1 部を検収用として添付すること。

(2) 最終納入物件

本仕様書で定義されたすべての機能を対象とする。

- 以下記載の文書等を収めた記録媒体(CD-R 又は DVD-R)一式
  - ① 暗号アルゴリズム実装試験ツール(JCATT)取扱説明書(日本語版及び英語版)
  - ② 暗号アルゴリズム実装試験仕様書
  - ③ JCATT ファイルフォーマット仕様書
  - ④ ②③の生成に必要な LaTeX ソースファイル
  - ⑤ テスト報告書、障害管理表(障害内容と対処内容の一覧表)
  - ⑥ 設計資料(基本設計書、詳細設計書)

⑦　納入物件一覧リスト及びソースコード一覧リスト

⑧　JCATT が入出力するファイルのサンプル

⑨　JCATT のソースコード及び実行形式生成に必要なファイル

⑩　JCATT の実行用ロードモジュール

⑪　JCATT 開発成果報告書及びその概要版

- 上記資料①～③、⑤～⑥、⑪の紙媒体各 1 部を検収用として添付すること。

(3) 納入物件作成にあたっての注意事項

①～③の作成にあたっては、次の点に留意すること。

- 用語の定義は、「暗号モジュール試験及び認証制度の基本規程（JCM-01)」(http://www.ipa.go.jp/security/jcmvp/documents/jcm01.pdf) による。
- 一般的に使用されている用語及び「暗号モジュール試験及び認証制度の基本規程（JCM-01)」において定義されている用語以外の用語を使用する際には、用語の定義を行い、その意味が明確になるように記述すること。

⑤の作成にあたっては、次の点に留意すること。

- テスト報告書は、十分なテスト項目とそのテスト内容、テスト手順及び判断基準の詳細を記述した文書であること。テストの手法、結果についても報告書に記載すること。
- 障害管理表には、テスト工程において発生した障害内容と、それに対する対処内容を具体的に記述すること。

⑪の作成にあたっては、次の点に留意すること。

- 本開発における成果の概要を対外的に説明できる文書であること。内容、分量については、過去の情報セキュリティ対策事業に関する開発成果報告書、成果概要報告書と同等以上のものとすること(http://www.ipa.go.jp/security/develop/software.html を参照)。

10.4. 検収条件

検収では、本仕様書の条件、項目が満たされているか否かにつき確認を行う。また、品質については、実際の暗号アルゴリズム実装試験の実行に耐え得るか否かを基準に判断し、確認を行う。

―以上―

「暗号アルゴリズム実装試験ツールの機能追加(GCM/XTS/鍵確立手法)」

入札資料作成要領及び評価手順

独立行政法人 **情報処理推進機構**

目　　次

第1章　入札者が提出すべき資料

第2章　提案書の作成要領及び説明

2.1　提案書の構成及び記載事項

2.2　プロジェクト計画案の作成方法

2.3　提案書様式

2.4　留意事項

第3章　添付資料の作成要領

3.1　個人情報保護体制についての記入方法

3.2　情報セキュリティ対策ベンチマーク確認書の記入方法

第4章　評価項目一覧の構成と記載要領

第5章　評価手順

5.1　落札方式

5.2　総合評価点の配分

5.3　技術審査

5.4　評価基準

5.5　配点構成

5.6　合否評価

5.7　技術点の算出

5.8　総合評価点の算出

第1章　入札者が提出すべき資料

入札者は、独立行政法人 情報処理推進機構（以下「機構」という。）が提示する資料を受け、下表に示す資料を作成し、機構へ提示する。

[入札者が機構に提示する資料]

資料名称	資料内容
①～⑤	委任状、入札書、納税証明書、登記簿謄本等及び提案書受理票。 詳しくは入札説明書を参照のこと。
⑥提案書 ⑦提案書(電子媒体)	仕様書に記述された要求仕様をどのように実現するかを説明したもの。主な項目は以下のとおり。 ・全体方針 ・情報システムの機能等に関する要件の実現方策 別紙：「プロジェクト計画案」にて作業の体制及び管理方法などについて記載すること。 作業の体制について、要員の暗号アルゴリズム実装に関する実績を記載する際には、当該暗号アルゴリズムを実装した製品に関する説明を含めること。
⑧添付資料	以下の資料を添付すること。 ・「個人情報保護体制について」 ・「情報セキュリティ対策ベンチマーク確認書」
⑨評価項目一覧	Ⅴ．評価項目一覧にて提示している、本件に係る提案をどのような観点・基準で評価するかを取りまとめた表。 評価項目一覧の提出にあたっては、提案書ページ番号欄に該当する提案書のページ番号を記入したものとすること。
⑩補足資料（任意提出）	入札者が作成した提案の詳細を説明するための資料。補足資料に記載されている内容は、直接評価されて点数が付与されることはない。 例：担当者略歴、会社としての実績、実施条件等

第2章　提案書の作成要領及び説明

2.1　提案書の構成及び記載事項

次表に、別添「評価項目一覧」から[提案書の目次]の大項目を抜粋したもの及び求められる提案要求事項の概要を示す。提案書は、当該「提案書の目次」に従い、提案要求内容を十分に咀嚼した上で実現可能な内容を記述すること。なお、目次及び要求事項の詳細は、別添「評価項目一覧」を参照すること。

[提案書目次]

提案書 目次項番	大項目	提案要求事項の概要説明
1	全体方針	目標設定、実施作業内容、開発プロセスについて
2	情報システムの機能等に関する要件の実現方策	技術的課題のある機能の実現方策
別紙	プロジェクト計画書案	本件を確実に実施するための、体制、要員、工程計画、工程管理計画、品質保証計画、セキュリティ計画などについて「プロジェクト計画書案」としてまとめたもの。詳細は、2.2プロジェクト計画案の作成方法を参照のこと。 注）この提案書別紙は、採点の対象となる。

2.2　プロジェクト計画案の作成方法

PMBOK等に基づいたプロジェクト計画書案を作成の上、提案書の別紙として提出すること。プロジェクト計画書案は、ひとつの独立したドキュメントとして成立するように構成し、章立てを提案書本文から引き継がずに最初から開始すること。

プロジェクト計画書案には、以下の内容が含まれていることを求める。提案書本文で記述した事項と重複することを妨げない。

また、機構側の体制等、提案時点で知り得ない情報を要するものについては、想定できる範囲内で記述すること。

① 実施体制
- ・作業要員等について、実働可能な人数と役割を含めて図表を用いた記述。
- ・特に異なる組織が含まれる場合（共同開発者、外注者等）には、それぞれの役割分担と関係。
- ・開発の一部を外注する場合、その作業内容。
- ・主要なリーダ/担当者について、担当作業、スキル、略歴
- ・社内外のセキュリティに関する教育の受講歴
- ・コミュニケーション計画及びプロジェクトの意思決定手順

② プロジェクトマネージャのスキル
- ・プロジェクトマネージャのシステム開発経験
- ・プロジェクトマネージャのPMBOK・EVMに基づいたプロジェクト管理の経験
- ・本プロジェクトのポイント、成功要因、リスクの分析

③ 工程計画（資源・工数・要員などの計画を含む）
- ・EVMに基づくWBS（ワーク・ブレークダウン・ストラクチャー）
- ・WBSは、少なくともレベル2、必要に応じてレベル3まで細分化するものとし、作業項目毎に工数もしくはコストを含めて記載
- ・主要なマイルストーンを設定してください。

④ 工程管理計画

・具体的な、WBSディクショナリーの骨子及び進捗評価基準（あるいはその考え方）

⑤ ドキュメント一覧

・納品物だけでなく、プロジェクト遂行にあたって用いるドキュメントを全て

⑥ 品質保証計画

・具体的な、ドキュメント作成基準の考え方、ドキュメントレビュー計画、品質評価指標の考え方など

なお、一部のドキュメントについて、発注仕様書において作成基準を指定している場合があるので注意すること。

⑦ セキュリティ計画

・実施体制、設計における情報セキュリティ対策の方針前提条件、制約条件及びリスク分析

2.3 提案書様式

① 提案書及び評価項目一覧はA4判にて印刷し、特別に大きな図面等が必要な場合には、原則としてA3判にて提案書の中に折り込む。

② 提案書については、電子媒体に保存された電子ファイルの提出を求める。その際のファイル形式は、原則として、Microsoft Office形式、OpenOffice形式またはPDF形式のいずれかとする（これに拠りがたい場合は、機構まで申し出ること）。記録媒体は、CD-RまたはDVD-Rとする。

2.4 留意事項

① 機構から連絡が取れるよう、提案書には連絡先（電話番号、FAX番号、及びメールアドレス）を明記する。

② 提案書を評価する者が特段の専門的な知識や商品に関する一切の知識を有しなくても評価が可能な提案書を作成する。なお、必要に応じて、用語解説などを添付する。

③ 入札者は、提案内容について具体的に提案書本文に記載すること。より具体的・客観的な詳細説明を行うための資料を、提案書本文との対応付けをした上で補足資料として提出することは可能であるが、その際、提案要求事項を満たしているかどうかが提案書本文により判断されることに留意すること。例えば、提案書本文に「補足資料〇〇参照」とだけ記載しているものは、提案書に具体的提案内容が記載されていないという評価となる。

④ 上記の提案書構成、様式及び留意事項に従った提案書ではないと機構が判断した場合は、提案書の評価を行わないことがある。また、補足資料の提出や補足説明等を求める場合がある。

⑤ 提案書、その他の書類は、本入札における総合評価落札方式の技術点評価にだけ使用する。ただし、落札者の提案書（別紙を除く）は契約書に添付する。

⑥ 提案書別紙「プロジェクト計画案」については、調整の後に合意形成するものとする。

第3章　添付資料の作成要領

3.1　個人情報保護体制についての記入方法

【様式-A】を用いて作成してください。

「ご回答者連絡先」を記入し、設問に回答（はい、いいえのいずれかを　○　で囲みください。）の上、必要事項の追加記入をお願い致します（※余白を縦横に伸縮してご記入ください）。

なお、本様式は、個人情報の取扱いに関して御社が講じている保護措置について確認することを目的としております。従いまして、設問は応募資格を定めているものではなく、回答の内容により直ちに失格となるということはありません。但し、プロジェクト計画の妥当性評価に用いる場合があります。

3.2　情報セキュリティ対策ベンチマーク確認書の記入方法

本件の担当部署を含む組織体を対象として、情報セキュリティ対策ベンチマーク（http://www.ipa.go.jp/security/benchmark/index.html）を実施いただき、その結果をご報告いただきます。【様式-B】に従い作成してください。

なお、本様式は、御社における情報セキュリティに対する取組について確認することを目的としております。従いまして、設問は応募資格を定めているものではなく、回答の内容により直ちに失格となるということはありません。但し、プロジェクト計画の妥当性評価に用いる場合があります。

第4章　評価項目一覧の構成と記載要領

評価項目一覧の構成及び概要説明を以下に記す。「提案書ページ番号」及び「遵守確認欄」については、【入札者が記載する欄】として記載要領をしめしている。

[評価項目一覧の構成と概要]

項目欄名		概要説明
提案書の目次		評価項目一覧の提案書の目次。提案書の構成は、評価項目一覧の構成と同一であること。
評価項目		評価の観点
評価区分	遵守確認事項(遵守)	本件を実施する上で遵守すべき事項。これら事項に係る内容の提案は求めず、当該項目についてこれを遵守する旨を記述する。
	提案要求事項(必須)	必ず提案するべき事項。これら事項については、入札者が提出した提案書について、各提案要求項目の評価基準に従い評価し、それに応じた得点配分の定義に従い採点する。 評価ランクDの提案は、不合格とする。
提案書ページ番号		【入札者が記載する欄】 作成した提案書における該当ページ番号を記載する。該当する提案書の頁が存在しない場合には空欄とする。評価者は、本欄に記載されたページを各提案要求事項に係る提案記述の開始ページとして採点を行う。
遵守確認欄		【入札者が記載する欄】 評価区分が「遵守確認事項(遵守)」の場合に、入札者は、遵守確認事項を実現・遵守可能である場合は○を、実現・遵守不可能な場合（実現・遵守の範囲等について限定、確認及び調整等が必要な場合等を含む）には×を記載する。
配点構成及び審査基準		評価区分が「提案要求事項(必須)」の評価項目に対して、どのような基準で採点するかを示している。

第5章　評価手順

5.1 落札方式

次の要件をともに満たしている者のうち、総合評価点のの最も高い者を落札者とする。

① 入札価格が予定価格の範囲内であること。

② 評価項目一覧に記載される評価項目において、「不合格」の項目が無いこと。

5.2 総合評価点の配分

総合評価点　＝　技術点　＋　価格点

技術点と価格点の配分は1:1とする。

5.3 技術審査

「V. 評価項目一覧」で示す、評価項目、評価基準、配点構成に基づき、技術審査を行う。

5.4 評価基準

各評価項目には、下表の評価指標に則った評価基準が具体的に設定されている。
この評価基準に基づき、審査員は合議制により各評価項目の評価ランクを決定する。
評価項目によっては、一部の評価ランクを適用しないことが予め決められている場合がある。

評価ランク	評価指標
S	通常の想定を超える卓越した提案内容であるなど。
A	通常想定される提案として、優位性のある内容である。
B	通常想定される提案としては妥当な提案であると認められる。
C	最低限の記述があると認められる。
D	内容が要件に対して不十分である、明らかに提案要求事項を満たさない、他の提案内容との間に看過できない矛盾がある、遵守確認事項との矛盾がある、あるいは記載がない。(不合格)

5.5 配点構成

評価項目毎に評価ランクに応じた得点が決定される。
各評価項目における配点構成は、「評価項目一覧」の「配点構成」欄にて定義されている。

5.6 合否評価

評価ランクDが設定されている評価項目について、評価ランクがDとなった場合には、不合格となる。入札者は、提案書にて要件を全て充足することを示さなければならない。一つでも要件が充足できないとみなされた場合は、その提案は不合格となる。

5.7 技術点の算出

ランクD（不合格）の評価が無い提案について、全ての評価項目における得点を合計し、これを技術点とする。

5.8 総合評価点の算出

以下を合計し、総合評価点を算出する。

① 「5.7 技術点の算出」により与えられる技術点

② 満点の場合の技術点 × (1 － 入札価格 ÷ 予定価格) により得た数値の小数点以下2位を切り捨てて算出した価格点

【様式-A】

個人情報保護体制について

本様式は、個人情報の取扱いに関して御社が講じている保護措置について確認することを目的としております。お手数ですが、最初に「ご回答者連絡先」を記入し、以下の設問に回答（はい、いいえのいずれかを〇で囲みください。）の上、必要事項の追加記入をお願い致します。

余白を縦横に伸縮してご記入ください。

ご回答者連絡先

組　　織　　名	
部　　署　　名	
氏　　名	
連絡先電話番号	
メールアドレス	

Ｑ１．個人情報保護に係るプライバシーポリシー・規程・マニュアルはございますか。

【　は　い　・　いいえ　】

「は　い」を○で囲んだ方は、以下の事項を記入してください。

以下に名称、作成年月日、作成の参考にした業界ガイドライン（名称・作成機関名）を記入してください。 **【個人情報保護に関するプライバシーポリシー・規程・マニュアル】**

Ｑ２．個人情報保護に係る組織内体制はありますか。

【　は　い　・　いいえ　】

「は　い」を○で囲んだ方は、以下の事項を記入してください。

以下に担当部門、役職名、役割、担当業務範囲を記入してください。 **【個人情報保護に係る組織内体制】**

Ｑ３．個人情報を取扱う従事者（派遣職員、アルバイトを含む）への教育・研修を実施しておりますか。

【　は　い　・　いいえ　】

「は　い」を○で囲んだ方は、以下の事項を記入してください。

以下に実施部門、開催時期・年間回数、対象者、使用テキストを記入してください。 **【個人情報保護に係る従事者への教育・研修体制】**

Ｑ４．個人情報保護に係る監査規程はありますか。　【　は　い　・　いいえ　】

「は　い」を○で囲んだ方は、以下の事項を記入してください。

以下に監査規程（名称、制定年月日）を記入してください。また、すでに監査の実績がある場合は、直近の監査実施日を記入してください。 **【個人情報保護に係る監査規程・直近の監査実施日】**

Ｑ５．情報処理システムの安全対策はありますか。　【　は　い　・　いいえ　】

「は　い」を○で囲んだ方は、以下の事項を記入してください。

【情報処理システムの安全対策】

「いいえ」と回答した設問に対して、このたびの IPA からの個人情報を取扱う業務を実施する上でご検討されている保護措置の案があれば以下にご記入ください。形式は自由です。余白を縦横に伸縮してご記入ください。

【今回の個人情報を取扱う業務でご検討されている保護措置案】

Ｑ６．認定団体からプライバシーマークを付与されておりますか。　【　は　い　・　いいえ　】

「は　い」を○で囲んだ方は、以下の事項を記入（上書き）してください。

認定番号：○○○○○○○ **有効期間：**○○○○**年**○○**月**○○**日　～　**○○○○**年**○○**月**○○**日**

【様式－B】

平成　　年　　月　　日

[会社名]
[責任者役職・氏名]

情報セキュリティ対策ベンチマーク確認書

情報セキュリティ対策ベンチマークを実施し、下記の評価結果に相違ないことを確認します。

記

1.確認日時

平成　　年　　月　　日 【実際に確認を行った日時】

2. 確認対象

【情報セキュリティ対策ベンチマークの確認を行った範囲について記載
（例、本件業務を請け負われる部署を含む組織体等の名称）】

3. 情報セキュリティ対策ベンチマーク実施責任者

【情報セキュリティ対策ベンチマークによる確認を実施した者。】

4. 確認結果

全項目に係る平均値：

なお、ベンチマーク実施出力結果を別紙として添付します。

V. 評価項目一覧

提案書の目次			評価項目	評価区分	提案書ページ番号	遵守確認欄	配点構成および評価基準				
大項目	中項目	小項目					S	A	B	C	D
1. 全体方針											
	1.1 開発プロセス										
		1.1.1	開発業務の範囲について、「開発業務内容」に記載している項目を一括して受託すること（部分についての提案は認めない）	遵守							
		1.1.2	全体プロセスの特徴、本件に採用した理由は明確かつ適切であるか。	必須			10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。 本件の状況を考慮して、開発プロセスに独自のカスタマイズがかけられているなど、本件に適用する理由と効果が明確になっている。	4 全体プロセスの特徴が記載されている。 社内規準あるいは業界規準に準拠している。	0 左記Bの基準を満たしていない。	不合格
		1.1.3	開発手法やテスト方法は具体的かつ実行可能であるか。 採用するプロジェクト管理ツールや開発支援ツールは適切であるか。	必須			10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。 選択された開発手法・テスト方法に合わせてプロジェクト管理ツールや開発支援ツールが仮定され、その選択理由や効果、選択したツールの導入実績についても説明されている。	4 本件の特徴を考慮して、採用する開発手法・テスト方法が選択されており、具体的かつ実行可能な内容となっている。	0 左記Bの基準を満たしていない。	不合格
2. 情報システムの機能等に関する要件の実現方策											
	2.1機能要件										
		2.1.1	Ⅲ 仕様書 に記載された機能要件を全て実現すること。	遵守							
3. 作業の体制及び管理（プロジェクト計画案）											
	3.1 実施体制										
		3.1.1	体制図は十分に詳細化され、開発、工程管理、品質保証、セキュリティ対策等の活動を適切に実施できるよう、役割・責任が明記されているか。 プロジェクトメンバーは、本件実施に十分な経験を持つことが説明されているか。	必須			10 右記Aの基準を満たしている。 詳細設計開始時点の構成要員は決定し、組織体制図に氏名あるいはそれに準ずる情報を明記している。	7 右記Bの基準を満たしている。 設計・開発、工程管理、品質保証、セキュリティ対策等の活動について役割分担がなされている。 プロジェクトメンバーは、上記の役割分担に応じた実務経験を有する。	4 提案する体制図において、各グループ及び構成要員の役割、責任を明確にしている。 プロジェクトメンバーの実務経験が記載されている。	0 左記Bの基準を満たしていない。	不合格
		3.1.2	プロジェクトメンバーの中に暗号技術に知見がある要員が含まれているか。（ヒアリングと合わせて評価を実施する予定）	必須			10 右記Aの基準を満たし、かつ、その経験が充実している。	7 右記Bの基準を満たしている。 暗号技術の適用/応用に係る実務を経験している。	4 暗号技術に知見がある要員が含まれている。	0 左記Bの基準を満たしていない。	不合格
		3.1.3	コミュニケーション計画及びプロジェクトの意思決定手順	必須			10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。 対象者の具体的な役職などに基づいて記載されている。	4 適切なコミュニケーション計画及びプロジェクトの意思決定手順が記載されている。	0 左記Bの基準を満たしていない。	不合格
	3.2 プロジェクトマネージャのスキル（ヒアリングと合わせて評価を実施する予定）										

	3.2.1	システム開発経験:プロジェクトマネージャーは、本件システムと同等規模(利用ユーザ数、トランザクション数、要求される信頼性等)のシステムの開発・運用をどれくらい実施した経験があるか。 プロジェクト経験については、成功したプロジェクトのみが記述されているか。また、その際、プロジェクトの成功を証明する資料を添付されているか。	必須			10 右記Aの基準を満たし、かつ、その能力が卓越している。	7 右記Bの基準を満たしている。 プレゼンテーションを通じて、自分のシステム開発に関する能力(知識・スキル・経験)を本プロジェクトで発揮できることを示している。	4 プロジェクトマネージャーは本件システムと同等規模のシステム開発プロジェクトの経験を5年以上有している。 プロジェクトマネージャーは、それらのプロジェクトの成功に貢献したポイントを提示している。	0 左記Bの基準を満たしていない。	不合格
	3.2.2	プロジェクトマネージャーは、PMBOK・EVMに基づいたプロジェクト管理の経験をどれくらい有しているか。 プロジェクト経験については、成功したプロジェクトのみが記述されているか。また、その際、プロジェクトの成功を証明する資料を添付されているか。	必須			10 右記Aの基準を満たし、かつ、その能力が卓越している。	7 右記Bの基準を満たしている。 プレゼンテーション/質疑応答を通じて、自分のPMBOK・EVMに関する能力(知識・スキル・経験)を発揮している。 プレゼンテーション/質疑応答を通じて、自分のプレゼンテーション力・質問対応力・課題に対する対応策を立案していく能力等を発揮している。	4 プロジェクトマネージャーはPMBOK・EVMに基づいたプロジェクト管理の経験を一通り(計画、実行、評価、改善)有していることが示されている。 プロジェクトマネージャーは、それらのプロジェクトマネジメントを成功させたことを提示している。	0 左記Bの基準を満たしていない。	不合格
	3.2.3	プロジェクトマネージャーは、本プロジェクトのポイントを明確に説明できるか。その内容は適切か。 プロジェクトマネージャーは、本プロジェクトにおける成功要因及びリスクを把握できているか。	必須			10 右記Aの基準を満たし、かつ、その能力が卓越している。	7 右記Bの基準を満たしている。 プレゼンテーション/質疑応答を通じて、自分のプロジェクトの深い理解度を発揮している。	4 提案書の中で。本プロジェクトのポイント・成功要因・リスクを端的に説明している。	0 左記Bの基準を満たしていない。	不合格
3.3 工程計画(資源・工数・要員などの計画を含む)										
	3.3.1	WBS単位にスケジュールが作成されているか。 作業項目の順序や依存関係は明確かつ適切に設定されているか。	必須			10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。 各WBSの作業順序や依存関係が整理され、手戻りがないように工夫を行っている。	4 WBSのタスク単位で、成果物作成に必要な工数を適切に見積もり、妥当なスケジュールを作成している。	0 左記Bの基準を満たしていない。	不合格
	3.3.2	WBS構造は発注者から提示された「WBSレベル」にしたがって設定されているか。 WBSは適切な単位のWPに分割されているか。	必須			10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。 WBSは適切な単位のWPに分割されており、かつ、詳細化が必要な部分については、適切なレベルで詳細化を行っている。	4 発注者から提示された「WBSレベル」にしたがってWBSが作成されている。	0 左記Bの基準を満たしていない。	不合格
	3.3.3	WBS単位でコスト(または工数)が明記されているか。 コスト全体に対する各WBSの配分は適切であり、また、リスクに応じたリザーブを適切に見込んでいるか。	必須			10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。 算出されたコストは、作業工数×人月単価によって、正確に見積もっている。	4 WBS単位でコスト(または工数)が明記され、配分は適切である。	0 左記Bの基準を満たしていない。	不合格
3.4 工程管理計画(WBSディクショナリ)										
	3.4.1	計測規準(進捗評価基準)の考え方が示されているか。その内容は適切か。	必須			10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。 作成終了をもって完了とせず、レビューや検証、検査に要する工程を見込んでいる。	4 成果物の種類ごとに、計測基準が定められている。	0 左記Bの基準を満たしていない。	不合格
	3.4.2	WBS単位の成果物は明確かつ適切に設定されているか。 成果物の記載内容が定義され、サンプル成果物などが具体的に示されているか。	必須			10 右記Aの基準を満たし、かつ、一般的でない中間成果物等について、サンプルが提示されている。	7 右記Bの基準を満たしている。 WBS単位の成果物に、納入物件以外の中間成果物等が適切に設定されている。	4 WBS単位の成果物は、少なくとも納入物件について明確に設定されている。	0 左記Bの基準を満たしていない。	不合格
3.5 ドキュメント一覧										
	3.5.1	納入物以外のドキュメント、管理台帳、連絡票などについて、網羅的に記述されているか。	必須			10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。 定義されたドキュメントの利用目的が端的に記載されている。	4 会議体に提出する資料、課題整理に用いる台帳、連絡書式など、プロジェクト遂行に必要なドキュメントが定義されている。	0 左記Bの基準を満たしていない。	不合格
3.6 品質保証計画										

	3.6.1	品質管理に必要と思われる体制、活動内容は具体的かつ実現可能であるか。	必須			10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。 提案する品質管理業務の活動を行った結果としての実効性について説明されている。	4 品質管理業務を適切に実施する為に必要となる品質管理体制、活動内容が具体的に記載され、かつ、実現可能であることが説明されている。	0 左記Bの基準を満たしていない。	不合格
	3.6.2	ドキュメント作成基準について、様式、書き方などの考え方が示されているか。当該基準は全社的（あるいはそれに匹敵する規模の組織、例えば事業所、事業部などにおける）基準に基づくなど、統一的なものか。	必須			10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。 社内規準などに基づく、雛形、作成基準が具体的に示されている。	4 ドキュメントの作成基準についての考え方が記載され、本プロジェクトのみに有効ではないことが示されている。	0 左記Bの基準を満たしていない。	不合格
	3.6.3	ドキュメントレビュー計画について、適切に詳細化されているか。 作成担当部門による自己評価のみで終わってしまうことはないか。	必須			10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。 社内規準などに基づいて、担当部署・グループ内でのレビューだけでなく、品質管理部門あるいは社外コンサルタントのレビューを受けることとなっているか。	4 ドキュメントのレビュー計画について、体制、コミュニケーション計画に記載されている内容が詳細化され、レビュー手順の考え方が記載されている。	0 左記Bの基準を満たしていない。	不合格
	3.6.4	品質評価のための指標・基準が提示されているか。それらの内容は適切か。	必須			10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。 社内規準などに基づいた具体的なが提示され、基準、目標値等が設定されている。	4 品質評価指標についての考え方が記載されている。	0 左記Bの基準を満たしていない。	不合格
	3.6.5	テスト方針、検証方法・指標、目標値に関して効果的かつ効率的な提案がなされている。目指すべき機能、性能等に対して、正しい目標値が設定されている。	必須			10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。 提案内容は、効果的かつ効率的である。	4 テスト方針、検証方法・指標、目標値に関して具体的な提案がなされている。目指すべき機能、性能等に対して、正しい目標値が設定されている。	0 左記Bの基準を満たしていない。	不合格
3.7 セキュリティ計画										
	3.7.1	実施体制における情報セキュリティ対策として、関連ドキュメントのアクセス管理、コーディング規約の制定などがなされているとともに、それらの効率的運用のための方策が計画されているか。	必須			10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。 それらの効率的運用のための方策が計画されている。	4 関連ドキュメントのアクセス管理、コーディング規約の制定などがなされている。	0 左記Bの基準を満たしていない。	不合格
	3.7.2	ソフトウェアの設計にあたり、その情報セキュリティに関する妥当性を確認するための設計レビューの範囲及び方法について、具体的に提案されているか。	必須			10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。 他のレビューから独立した計画となっており、それらの効率的運用のための方策が計画されている。	4 情報セキュリティに関連する機能・性能等に関するレビューの計画について、その範囲及び方法が具体的に記載されている。	0 左記Bの基準を満たしていない。	不合格